RESEARCH CENTER
Paris

FIELD

Activity Report 2019

Section Partnerships and Cooperations

Edition: 2020-03-21

ALMANACH Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- **ANR SoSweet** (2015-2019, PI J.-P. Magué, resp. ALMAnaCH: DS; Other partners: ICAR [ENS Lyon, CRNS], Dante [Inria]). Topic: studying sociolinguistic variability on Twitter, comparing linguistic and graph-based views on tweets
- **ANR ParSiTi** (2016-2021, PI Djamé Seddah, Other partners: LIMSI, LIPN). Topic: context-aware parsing and machine translation of user-generated content
- **ANR PARSE-ME** (2015-2020, PI. Matthieu Constant, resp. Marie Candito [ALPAGE, then LLF], ALMAnaCH members are associated with Paris-Diderot's LLF for this project). Topic: multi-word expressions in parsing
- **ANR Profiterole** (2016-2020, PI Sophie Prévost [LATTICE], resp. Benoit Crabbé [ALPAGE, then LLF], ALMAnaCH members are associated with Paris-Diderot's LLF for this project). Topic: modelling and analysis of Medieval French
- **ANR TIME-US** (2016-2019, PI Manuela Martini [LARHRA], ALMAnaCH members are associated with Paris-Diderot's CEDREF for this project). Topic: Digital study of remuneration and time budget textile trades in XVIIIth and XIXth century France
- **ANR BASNUM** (2018-2021, PI Geoffrey Williams [Université Grenoble Alpes], resp. ALMAnaCH: LR). Topic: Digitalisation and computational linguistic study of Basnage de Beauval's *Dictionnaire universel* published in 1701.

9.1.2. Competitivity Clusters and Thematic Institutes

- **PRAIRIE institute** (2019-2024, Dir.: Isabelle Ryl). Benoît Sagot was granted a Chair in this newly created research institute dedicated to Artificial Intelligence.
- **GDR LiFT** (2019-): LiFT is a CNRS-funded national coordination structure (GDR) involving many French teams involved in computational, formal and descriptive linguistics, in order to facilitate the emergence of fruitful collaborations. ALMAnaCH is involved in the GDR.
- **LabEx EFL** (2010-2019, PI Christian Puech [HTL, Paris 3], Sorbonne Paris Cité). Topic: empirical foundations of linguistics, including computational linguistics and natural language processing. ALPAGE was one of the partner teams of this LabEx, which gathers a dozen of teams within and around Paris whose research interests include one aspects of linguistics or more. BS serves as deputy head (and former head) of one of the scientific strands of the LabEx, namely strand 6 dedicated to language resources. BS and DS are in charge of a number of scientific "operations" within strands 6, 5 ("computational semantic analysis") and 2 ("experimental grammar"). BS, EVdLC and DS are now individual members of the LabEx EFL since 1st January 2017, and BS still serves as the deputy head of strand 6. Main collaborations are on language resource development (strands 5 and 6), syntactic and semantic parsing (strand 5, especially with LIPN [CNRS and U.Paris 13]) and computational morphology (strands 2 and 6, especially with CRLAO [CNRS and Inalco]).

9.1.3. Other National Initiatives

- **LECTAUREP project** (2017-2019): A preliminary study has been launched in collaboration with the National Archives in France, in the context of the framework agreement between Inria and the Ministry of Culture, to explore the possibility of extracting various components from digitised 19th Century notary registers.

- **Nénufar (DGLFLF - Délégation générale à la langue française et aux langues de France)**: The projects is intended to digitize and exploit the early editions (beginning of the 20th Century) of the Petit Larousse dictionary. ALMAnaCH is involve to contribute to the automatic extraction of the dictionary content by means of GROBID-Dictionaries and define a TEI compliant interchange format for all results.
- **PIA Opaline** (2017-2020): The objective of the project is to provide a better access to published French literature and reference material for visually impaired persons. Financed by the Programme d'Investissement d'Avenir, it will integrate technologies related to document analysis and re-publishing, textual content enrichment and dedicated presentational interfaces. Inria participate to deploy the GROBID tool suite for the automatic structuring of content from books available as plain PDF files.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- **H2020 Parthenos** (2015-2019, PI Franco Niccolucci [University of Florence]; LR is a work package coordinator) Topic: strengthening the cohesion of research in the broad sector of Linguistic Studies, Humanities, Cultural Heritage, History, Archaeology and related fields through a thematic cluster of European Research Infrastructures, integrating initiatives, e-infrastructures and other world-class infrastructures, and building bridges between different, although tightly interrelated, fields.
- **H2020 EHRI** "European Holocaust Research Infrastructure" (2015-2019, PI Conny Kristel [NIOD-KNAW, NL]; LR is task leader) Topic: transform archival research on the Holocaust, by providing methods and tools to integrate and provide access to a wide variety of archival content.
- **H2020 Iperion CH** (2015-2019, PI Luca Pezzati [CNR, IT], LR is task leader) Topic: coordinating infrastructural activities in the cultural heritage domain.
- **H2020 HIRMEOS**: HIRMEOS objective is to improve five important publishing platforms for the open access monographs in the humanities and enhance their technical capacities and services and rendering technologies, while making their content interoperable. Inria is responsable for improving integrating the entity-fishing component deplyed as an infrastructural service for the five platforms.
- **H2020 DESIR**: The DESIR project aims at contributing to the sustainability of the DARIAH infrastructure along all its dimensions: dissemination, growth, technology, robustness, trust and education. Inria is responsable for providing of a portfolio of text analytics services based on GROBID and entity-fishing.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

- **ERIC DARIAH "Digital Research Infrastructure for the Arts and Humanities"** (set up as a consortium of states, 2014-2034; LR served president of the board of director until August 2018) Topic: coordinating Digital Humanities infrastructure activities in Europe (17 partners, 5 associated partners).
- **COST enCollect** (2017-2020, PI Lionel Nicolas [European Academy of Bozen/Bolzano]) Topic: combining language learning and crowdsourcing for developing language teaching materials and more generic language resources for NLP

9.2.3. Collaborations with Major European Organizations

Collaborations with institutions not cited above (for the SPMRL initiative, see below):

- Berlin-Brandenburgische Akademie der Wissenschaften [Berlin-Brandenburg Academy of Sciences and Humanities], Berlin, Germany (Alexander Geyken) [lexicology]
- Österreichische Akademie der Wissenschaften [Austrian Academy of Sciences], Vienna, Austria (Karlheinz Moerth) [lexicology]

- Bar Ilan University (Yoav Goldberg, Hila Gonen) [non-canonical text processing]
- Dublin City University, Ireland (Teresa Lynn) [low-resource languages, user-generated content]
- University of Sheffield, United Kingdom (Lucia Specia, Carolina Scarton, Fernando Alva-Manchego) [text simplification]
- Univerza v Ljubljani [University of Ljubljana], Ljubljana, Slovenia (Darja Fišer) [wordnet development]

9.3. International Initiatives

9.3.1. Participation in Other International Programs

ANR-NSF project MCM-NL "Petit Prince" (2016-2020, PI John Hale [Cornell University, USA], resp. for Inria Paris/ALMAnaCH: Éric de La Clergerie) Topic: exploring correlations between data from neuro-imagery (fMRI, EEG) and data from NLP tools (mostly parsers). The data will come from "Le Petit Prince" read in French and English, and parsed with different parsers. Other partners: Cornell Univ., Univ. Michigan, Paris Saclay/Neurospin, Univ. Paris 8. Grant for ALMAnaCH: 108,500 euros

PHC Maïmonide (2018-2019, PI Djamé Seddah, co-PI Yoav Goldberg [Bar Ilan University]). Topics: Building NLP resources for analysing reactions to major events in Hebrew and French social media. Amount of the grant for the French side: 59,000 euros (89,000 euros for the whole project).

ALPINES Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

GIS, Géosciences franciliennes: scientific collaboration network between ten public institutions from the Paris (Ile-de-France) region, focused on natural resources and environment. The project-team Alpines is a member.

9.2. National Initiatives

9.2.1. ANR

9.2.1.1. B3DCMB

ANR Decembre 2017 - Novembre 2021 This project is in the area of data analysis of cosmological data sets as collected by contemporary and forthcoming observatories. This is one of the most dynamic areas of modern cosmology. Our special target are data sets of Cosmic Microwave Background (CMB) anisotropies, measurements of which have been one of the most fruitful of cosmological probes. CMB photons are remnants of the very early evolution of the Universe and carry information about its physical state at the time when the Universe was much younger, hotter and denser, and simpler to model mathematically. The CMB has been, and continue to be, a unique source of information for modern cosmology and fundamental physics. The main objective of this project is to empower the CMB data analysis with novel high performance tools and algorithms superior to those available today and which are capable of overcoming the existing performance gap. Partners: AstroParticules et Cosmologie Paris 7 (PI R. Stompor), ENSAE Paris Saclay.

9.2.1.2. ANR Cine-Para

October 2015 - September 2019, Laura Grigori is Principal Coordinator for Inria Paris. Funding for Inria Paris is 145 Keuros. The funding for Inria is to combine Krylov subspace methods with parallel in time methods. Partners: University Pierre and Marie Curie, J. L. Lions Laboratory (PI Y. Maday), CEA, Paris Dauphine University, Paris 13 University.

9.2.1.3. Non-local DD

ANR appel à projet générique October 2015 - September 2020

This project in scientific computing aims at developing new domain decomposition methods for massively parallel simulation of electromagnetic waves in harmonic regime. The specificity of the approach that we propose lies in the use of integral operators not only for solutions local to each subdomain, but for coupling subdomains as well. The novelty of this project consists, on the one hand, in exploiting multi-trace formalism for domain decomposition and, on the other hand, considering optimized Schwarz methods relying on Robin type transmission conditions involving quasi-local integral operators.

9.2.1.4. Soilμ-3D

ANR appel à projet générique October 2015 - april 2019

In spite of decades of work on the modeling of greenhouse gas emission such as CO2 and N2O and on the feedback effects of temperature and water content on soil carbon and nitrogen transformations, there is no agreement on how these processes should be described, and models are widely conflicting in their predictions. Models need improvements to obtain more accurate and robust predictions, especially in the context of climate change, which will affect soil moisture regime.

The goal of this new project is now to go further using the models developed in MEPSOM to upscale heterogeneities identified at the scale of microbial habitats and to produce macroscopic factors for biogeochemical models running at the field scale.

To achieve this aim, it will be necessary to work at different scales: the micro-scale of pores (μm) where the microbial habitats are localized, the meso-scale of cores at which laboratory measurements on CO2 and N2O fluxes can be performed, and the macro-scale of the soil profile at which outputs are expected to predict greenhouse gas emission. The aims of the project are to (i) develop new descriptors of the micro-scale 3D soil architecture that explain the fluxes measured at the macro-scale, (ii) Improve the performance of our 3D pore scale models to simulate both micro-and meso- scales at the same time. Upscaling methods like "homogeneization" would help to simulate centimeter samples which cannot be achieved now. The reduction of the computational time used to solve the diffusion equations and increase the number of computational units, (iii) develop new macro-functions describing the soil micro-heterogeneity and integrate these features into the field scale models.

9.2.1.5. Muffin

ANR appel à projet générique 2019.

S. Hirstoaga and P.-H. Tournier are members of the project MUFFIN, whose objective is to explore and optimize original computational scenarios for multi-scale and high dimensional transport codes, with priority applications in plasma physics. Several approximation methods are planed to be developed. It is at the frontier of computing and numerical analysis and intends to reduce the computational burden in the context of intensive calculation. Principal Investigator: B. Després (Sorbonne University).

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. NLAFET (197)

Title: Parallel Numerical Linear Algebra for Future Extreme-Scale Systems

Programm: H2020

Duration: November 2015 - April 2019

Coordinator: UMEÅ Universitet

Partners:

Science and Technology Facilities Council (United Kingdom)

Computer Science Department, UmeåUniversitet (Sweden)

Mathematics Department, The University of Manchester (United Kingdom)

Inria, Alpines group

Inria contact: Laura Grigori

The NLAFET proposal is a direct response to the demands for new mathematical and algorithmic approaches for applications on extreme scale systems, as identified in the FETHPC work programme and call. This project will enable a radical improvement in the performance and scalability of a wide range of real-world applications relying on linear algebra software, by developing novel architecture-aware algorithms and software libraries, and the supporting runtime capabilities to achieve scalable performance and resilience on heterogeneous architectures. The focus is on a critical set of fundamental linear algebra operations including direct and iterative solvers for dense and sparse linear systems of equations and eigenvalue problems. Achieving this requires a co-design effort due to the characteristics and overwhelming complexity and immense scale of such systems. Recognized experts in algorithm design and theory, parallelism, and auto-tuning will work together to explore and negotiate the necessary tradeoffs. The main research objectives are: (i) development of novel algorithms that expose as much parallelism as possible, exploit heterogeneity, avoid communication bottlenecks, respond to escalating fault rates, and help meet emerging power constraints; (ii) exploration of advanced scheduling strategies and runtime systems focusing on the extreme scale and strong scalability in multi/many-core and hybrid environments; (iii) design and evaluation of novel strategies and software support for both offline and online auto-tuning. The

validation and dissemination of results will be done by integrating new software solutions into challenging scientific applications in materials science, power systems, study of energy solutions, and data analysis in astrophysics. The deliverables also include a sustainable set of methods and tools for cross-cutting issues such as scheduling, auto-tuning, and algorithm-based fault tolerance packaged into open-source library modules.

9.3.1.2. ERC Synergy grant EMC2

Title: Extreme-scale Mathematically-based Computational Chemistry (EMC2)

Programm: ERC

Duration: September 2019 - August 2025

PIs: E. Cances (ENPC), L. Grigori (Inria), Y. Maday (Sorbonne University), J. P. Piquemal (Sorbonne University)

Molecular simulation is one of the most dynamic areas of scientific computing. Its field of application is very broad, ranging from theoretical chemistry and drug design to materials science and nanotechnology. Its importance in modern science has been acknowledged by two Nobel Prizes (Kohn & Pople in 1998; Karplus, Levitt & Warshel in 2013). It is also a gold mine of exciting problems for mathematicians and computer scientists.

Molecular simulation can be used as a virtual microscope to study more or less complex molecules with atomic-scale space-time resolution. It can also be used as a tool for computer-aided design (CAD) and the engineering of new molecules, materials and nano-devices.

However, molecular simulation still has important limitations. In particular, the simulation of very large molecular systems, or smaller systems in which electrons interact strongly with each other, remains out of reach today. Overcoming these limitations is extremely difficult. This requires joint breakthroughs in several disciplines, and can, in our opinion, only be achieved through an intensive multidisciplinary effort such as those made possible by ERC-Synergy-type funding.

Our objective is to overcome some of the current limitations in this field and to provide academic communities and industrial companies with new generation, dramatically faster and quantitatively reliable molecular simulation software, to enable those communities to address major technological and societal challenges of the 21st century (in health, energy, and the environment, for example).

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

- J. Demmel, UC Berkeley, USA
- M. Grote, Université de Bâle, Suisse
- F. Assous, Israel
- K.-M. Perfekt, Reading, UK
- T. Chacon, Seville, Spain

9.5. International Research Visitors

9.5.1. Visits to International Teams

9.5.1.1. Research Stays Abroad

- Visit of Laura Grigori to the group of J. Demmel at U.C. Berkeley, july-august 2019.

ANGE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR MFG (2016-2021)

Participant: Julien Salomon.

Project acronym: MFG

Project title: Mean Field Games

Coordinator: Sébastien Boyaval (LHSV/ENPC)

Funding: 299 160 euros.

Mean field game theory (MFG) is a new and active field of mathematics, which analyses the dynamics of a very large number of agents. Introduced about ten years ago, MFG models have been used in different fields: economics, finance, social sciences, engineering,... MFG theory is at the intersection of mean field theory, mathematical game theory, optimal control, stochastic analysis, variation calculation, partial differential equations and scientific calculation. Drawing on an internationally recognized French team on the subject, the project seeks to obtain major contributions in 4 main directions: the "medium field" aspect (i.e., how to obtain macroscopic models from microscopic models); the analysis of new MFG systems; their numerical analysis; the development of new applications. In this period of rapid expansion of MFG models, the project seeks to foster French leadership in the field and attract new researchers from related fields.

9.1.2. ANR INFAMIE (2015-2019)

Participant: Boris Haspot.

Program: ANR Défi de tous les savoirs (DS10) 2015

Project acronym: INFAMIE

Project title: INhomogeneous Flows : Asymptotic Models and Interfaces Evolution

Coordinator: Raphaël Danchin (Univ. Paris-Est)

Funding: 232 960 euros.

Our project aims at a better mathematical understanding of several models for the evolution of inhomogeneous flows. Through three main lines of research (see below), we will pursue a twofold final objective. First, we want to develop the current theory of regular solutions for several equations for the evolution of fluids, proposing a new approach and developing tools that are likely to be efficient in various areas of PDEs. Second, for a few selected concrete systems that describe flows in the earth environment or in astrophysics, we wish to use this general approach to extract as much information as possible concerning the qualitative behavior of the solutions.

9.1.3. ANR SEDIFLO (2015-2019)

Participants: Emmanuel Audusse, Martin Parisot.

Program: ANR Défi 1 “Gestion sobre des ressources et adaptation au changement climatique” (JCJC)

Project acronym: SEDIFLO

Project title: Modelling and simulation of solid transport in rivers

Coordinator: Sébastien Boyaval (LHSV/ENPC)

Based on recent theoretical and experimental results, this project is aimed at modelling transport of sediments within rivers. It will rely on innovations from the point of view of rheology as well as advanced mathematical tools (asymptotic model reduction, PDE discretisation).

9.1.4. ANR Hyflo-Eflu (2016-2019)

Participants: Jérémy Ledoux, Martin Parisot, Jacques Sainte-Marie, Julien Salomon.

ANR project call: Energies marines renouvelables

Project acronym: Hyflo-Eflu

Project title: Hydroliennes flottantes et énergie fluviale

Coordinator: Julien Salomon

The project is a collaboration between the Inria-team ANGE, specialist of free surface flow and optimisation, and the industrial developers of the turbine, HydroTube Energie. The objective of the project HyFlo-EFlu is to deliver a numerical software able to simulate the dynamic of a floating water turbine in real context. For the academic partner, the main challenge is in the simulation of the floating structure at the scale of the river, and the modelling of the vertical and horisontal axis turbine. For the industrial partner, the objective is the validation of the stability of the structure and the performance in term of energy production.

9.1.5. ANR CHARMS (2016-2020)

Participant: Cindy Guichard.

ANR project call: Transformations et inter-conversions énergétiques

Project acronym: CHARMS

Project title: Modèles de réservoirs quantitatifs pour les systèmes hydrothermaux complexes

Coordinator: Simon Lopez (BRGM)

Funding: 73k euros for LJLL (in 767k euros for the whole project)

CHARMS ANR project is focused on the mathematical methods and software tools dedicated to the simulation of the physical models issued from geothermal engineering. The final objective is the achievement of a highly parallel code, validated on realistic cases.

9.1.6. GdR EGRIN (2017–2021)

Participants: Emmanuel Audusse, Bernard Di Martino, Nicole Goutal, Cindy Guichard, Anne Mangeney, Martin Parisot, Jacques Sainte-Marie.

EGRIN stands for Gravity-driven flows and natural hazards. J. Sainte-Marie is the head of the scientific committee of this CNRS research group and A. Mangeney is a member of the committee. Other members of the team involved in the project are local correspondents. The scientific goals of this project are the modelling, analysis and simulation of complex fluids by means of reduced-complexity models in the framework of geophysical flows.

9.1.7. ANR FireCaster (2017-2020)

Participants: Frédéric Allaire, Vivien Mallet.

ANR project call: DS0104

Project acronym: FireCaster

Project title: Plateforme de prévision incendie et de réponse d'urgence

Coordinator: Jean-Baptiste Filippi (Univ. Corse)

Funding: 442k euros

The goal of the FireCaster project is to prototype a fire decision support system at the national scale to estimate upcoming fire risk (H+24 to H+48) and in case of crisis, to predict fire front position and local pollution (H+1 to H+12).

9.1.8. ANR CENSE (2017-2020)

Participants: Antoine Lesieur, Vivien Mallet.

ANR project call: DS0601

Project acronym: CENSE

Project title: Caractérisation des environnements sonores urbains : vers une approche globale associant données libres, mesures et modélisations

Coordinator: Judicaël Picaut (IFSTTAR)

Funding: 856k euros

The CENSE project aims at proposing a new methodology for the production of more realistic noise maps, based on an assimilation of simulated and measured data through a dense network of low-cost sensors.

9.1.9. ANR RAVEX (2017-2020)

Participant: Anne Mangeney.

ANR project call: DS0106

Project acronym: RAVEX

Project title: Développement d'une approche intégrée pour la réduction des Risques Associés au Volcanisme EXplosif, de la recherche sur l'aléa aux outils de gestion de crise : le cas de la Martinique

Coordinator: Olivier Roche (IRD)

Funding: 619k euros

9.1.10. ANR CINE-PARA (2015-2019)

Participant: Julien Salomon.

ANR project call: DS0708

Project acronym: CINE-PARA

Project title: Méthodes de parallélisation pour cinétiques complexes

Coordinator: Yvon Maday (LJLL)

9.1.11. PGMO Project ORACLE (2019-2021)

Participant: Julien Salomon.

PGMO Call

Project acronym: Oracle

Project title: Optimal Resource Allocation in micro-organisms under Changing Environment

Coordinator: Térence Bayen

9.2. European Initiatives

9.2.1.

Participants: Martin Parisot, Yohan Penel, Jacques Sainte-Marie.

CNRS PICS NHML (2017-2019)

Program: CNRS PICS (projet international de collaboration scientifique)

Project acronym: NHML

Project title: non-hydrostatic multilayer models

Duration: 01/17-12/19

Coordinator: Yohan Penel (Inria)

Other partners: IMUS (Sevilla, Spain)

Other Participants: Enrique Fernández-Nieto (Sevilla), Tomas Morales de Luna (Cordoba)

Funding: 12k euros

Abstract: This collaboration aims at designing a hierarchy of multilayer models with a non-hydrostatic pressure as a discretisation along the vertical axis of the Euler equations. The hierarchy relies on the degree of approximation of the variables discretised with a Discontinuous Galerkin method for the vertical direction. These innovative models will imply a theoretical study and the development of numerical tools in dimensions 1 and 2 before the modelling of other physical phenomena (viscosity effects, ...).

9.3. International Initiatives

9.3.1. Inria International Partners

Three long-term collaborations with foreign colleagues have to be mentioned:

- **Spain** - A collaboration with spanish researchers has been initiated in 2016 to derive accurate models and effecient algorithms for free surface flows including non-hydrostatic effects.
- **Germany** A collaboration with researchers from the University of Constance is in progress about domain decomposition and identifaction algorithms (G. Ciaramella, S. Volkwein). The internship (Masterarbeit) of S. Buchwald has been co-supervised by J. Salomon.
- **Hong-Kong, Switzerland** A collaboration with F. Kwok and M. Gander on time parallelization for assimilation algorithm is in progress. A first paper has been submitted in october.

9.4. International Research Visitors

- Y. Penel made two two-week stay (March, October) at the university of Sevilla (Spain) to collaborate with E. Fernández-Nieto.
- M. Parisot spent two months (October, November) at the university of Aachen (Germany) to collaborate with S. Noelle.

9.4.1. Visits of International Scientists

- G. Ciaramella (Constance University) visited J. Salomon (20.05-23.05) to work on algorithms related to design of experiments and identification.
- F. Kwok (Baptist University, Hong-Kong) visited J. Salomon (8.07-11.07) to work on algorithms related to time parallelization for identification.

ANTIQUE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. AnaStaSec

Title: Static Analysis for Security Properties

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2015 - September 2019

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.

9.1.2. DCore

Title: DCore - Causal Debugging for Concurrent Systems

Type: ANR générique 2018

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: March 2019 - February 2023

Coordinator: Inria Grenoble - Rhône-Alpes (France)

Others partners: IRIF (France), Inria Paris (France)

Inria contact: Jérôme Feret

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

Abstract: As software takes over more and more functionalities in embedded and safety-critical systems, bugs may endanger the safety of human beings and of the environment, or entail heavy financial losses. In spite of the development of verification and testing techniques, debugging still plays a crucial part in the arsenal of the software developer. Unfortunately, usual debugging techniques do not scale to large concurrent and distributed systems: they fail to provide precise and efficient means to inspect and analyze large concurrent executions; they do not provide means to automatically reveal software faults that constitute actual causes for errors; and they do not provide succinct and relevant explanations linking causes (software bugs) to their effects (errors observed during execution).

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.

Briefly, the causal debugging technology developed by the DCore project 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.

The project will build its causal debugging technology on results obtained by members of the team, as part of the past ANR project REVER, on the causal semantics of concurrent languages, and the semantics of concurrent reversible languages, as well as on recent works by members of the project on abstract interpretation, causal explanations and counterfactual causal analysis.

The project primarily targets multithreaded, multicore and multiprocessor software systems, and functional software errors, that is errors that arise in concurrent executions because of faults (bugs) in software that prevents it to meet its intended function. Distributed systems, which can be impacted by network failures and remote site failures are not an immediate target for DCore, although the technology developed by the project should constitute an important contribution towards full-fledged distributed debugging. Likewise, we do not target performance or security errors, which come with specific issues and require different levels of instrumentation, although the DCore technology should prove a key contribution in these areas as well.

9.1.3. REPAS

The project REPAS, Reliable and Privacy-Aware Software Systems via Bisimulation Metrics (coordination Catuscia Palamidessi, Inria Saclay), aims at investigating quantitative notions and tools for proving program

correctness and protecting privacy, focusing on bisimulation metrics, the natural extension of bisimulation on quantitative systems. A key application is to develop mechanisms to protect the privacy of users when their location traces are collected. Partners: Inria (Comete, Focus), ENS Cachan, ENS Lyon, University of Bologna.

9.1.4. SAFTA

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

Type: ANR JCJC 2018

Duration: February 2018 - August 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.

9.1.5. TGFSYSBIO

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

Type: Plan Cancer 2014-2019

Duration: December 2015 - September 2019

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.

9.1.6. 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.

9.2. European Initiatives

9.2.1. 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.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

Xavier Rival has a long standing collaboration with Bor-Yuh Evan Chang (University of Colorado, Boulder, USA), on the abstraction of symbolic properties and of complex memory data-structures.

Xavier Rival has a long standing collaboration with Sukyoung Ryu (KAIST, Daejeon, South Korea), on the analysis of dynamic programming languages. Xavier Rival has a set up a collaboration with Hongseok Yang (KAIST, Daejeon, South Korea), on the verification of probabilistic programs such as programs built in the Pyro framework.

Xavier Rival has started a collaboration with Shinya Katsumata, Jérémy Dubut, and Ichiro Hasuo (NII, Tokyo, Japan) on the formalization of abstract domains.

Xavier Rival has been working with Kwangkeun Yi on the writing of a book that should serve as an introduction to the field of static analysis, for students and engineers.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Internships

Marc Chevalier and Jérôme Feret have supervised the L3 internship of Jérôme Boillot (L3 at ENS Lyon).

Jérôme Feret has ksupervised the M2 internship of Yvan Sraka (M2 UPMC).

Xavier Rival has supervised M1 Internships of Guillaume Reboullet and of Luc Chabassier (M1 at DIENS).

Xavier Rival has supervised M2 Internships of Josselin Giet (MPRI at ENS) and of Vincent Rébiscoul (M2 at ENS Lyon).

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Xavier Rival has visited KAIST and Seoul National University in November 2019.

ARAMIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. Health Data Hub

Participant: Stanley Durrleman.

Project acronym: Precise-PD-HDH

Project title: Modélisation et prédiction de la progression de la maladie de Parkinson

Duration: 1 year (pilot project)

Coordinator: Jean-Christophe Corvol

Other partners: Inserm, réseau NS-PARK, ICM

9.1.2. ANR

9.1.2.1. ANR-NIH-NSF CANDT

Participant: Fabrizio de Vico Fallani [Correspondant].

Project acronym: CANDT

Project title: Advancing neuroscientific discovery and training by lowering the barrier of entry to network neuroscience via open science

Duration: Oct 2019 - Sep 2023

Amount: 137k€

Coordinator: Fabrizio De Vico Fallani

Other partners: Indiana Univ., US; UPenn, US

Abstract: This project will use open science methods and cloud-computing, effectively lowering the barrier of entry to network neuroscience and increase the widespread availability of well-maintained and reproducible network neuroscience tools. We will use the platform brainlife.io as a digital marketplace for network neuroscience analysis methods; network neuroscience tools and software will be packaged into self-contained, standardized, reproducible Apps, shared with and modified by a burgeoning community of users, and seamlessly integrated into existing brainlife.io processing and analysis pipelines. This approach will engage both experts in network science, scientists from other domains, and users of the proposed methods. In addition, it will ensure correct implementation, a high level of reproducibility, and maximal reusability of network neuroscience methods. As a requirement, Apps will also be accompanied by links to primary sources, in-depth tutorials, and documentation, and worked-through examples, highlighting their correct usage and offering solutions for mitigating possible pitfalls. This proposed research lowers the barrier of entry to network neuroscience, standardizes the software sharing process, and provides a cloud-based repository of expertly-maintained network neuroscientific tools and software that is made available to the broader neuroscientific community.

9.1.2.2. ANR-NIH-NSF NETBCI

Participants: Fabrizio de Vico Fallani [Correspondant], Mario Chavez, Denis Schwartz.

Project acronym: NETBCI

Project title: Modeling and predicting brain-computer interface learning from dynamic networks

Duration: Avr 2016 - Avr 2020

Amount: 322k€

Coordinator: Fabrizio De Vico Fallani

Other partners: Complex system group, UPenn, USA

Abstract: This project will bring together expertise in computational and experimental neuroscience, signal processing and network science, statistics, modeling and simulation, to establish innovative methods to model and analyze temporally dynamic brain networks, and to apply these tools to develop predictive models of brain-computer interface (BCI) skill acquisition that can be used to improve performance. Leveraging experimental data and interdisciplinary theoretical techniques, this project will characterize brain networks at multiple temporal and spatial scales, and will develop models to predict the ability to control the BCI as well as methods to engineer BCI frameworks for adapting to neural plasticity. This project will enable a comprehensive understanding of the neural mechanisms of BCI learning, and will foster the design of viable BCI frameworks that improve usability and performance.

9.1.2.3. ANR-NIH-NSF HIPLAY7

Participants: Olivier Colliot [Correspondant], Marie Chupin, Stanley Durrleman, Anne Bertrand.

Project acronym: HIPLAY7

Project title: Hippocampal layers: advanced computational anatomy using very high resolution MRI at 7 Tesla in humans

Duration: Jan 2017 - Jan 2020

Amount: 770k€

Coordinator: Olivier Colliot and Pierre-François Van de Moortele

Other partners: University of Minnesota, Neurospin

Abstract: The overall goal of this proposal is to develop a coherent mathematical framework for computational anatomy of the internal structures of the hippocampus based on cutting edge MRI acquisition techniques at 7 Tesla. These mathematical and computational approaches are expected to significantly advance the field of computational anatomy of the human brain, breaking down the millimeter barrier of conventional brain morphometry and providing a coherent analysis framework for anatomical data at ultra-high spatial resolution.

9.1.2.4. ANR PREV-DEMALS

Participants: Olivier Colliot [Correspondant], Marie Chupin, Stanley Durrleman, Anne Bertrand.

Project acronym: PREV-DEMALS

Project title: Predict to prevent frontotemporal lobar degeneration (FTLD) and amyotrophic lateral sclerosis (ALS)

Duration: Avr 2015 - Avr 2019

Amount: 487k€

Coordinator: Isabelle Le Ber

Other partners: ICM, AP-HP, CHR de Lille, CHU Limoges, CHU Rouen, Laboratory of Biomedical Imaging

Abstract: The project focuses on C9ORF72, the most frequent genetic form of frontotemporal lobar degeneration (FTLD) and amyotrophic lateral sclerosis (ALS). Since 2006, major discoveries have helped elucidate the pathological bases and linked FTLD and ALS: 1) TDP-43 aggregates in neurons and 2) C9ORF72 mutations in both disorders. Two major pathological subtypes are now defined in FTLD, FTLD-TDP and FTLD-TAU. C9ORF72 mutations (associated to FTLD-TDP) are the most frequent genetic causes of FTLD (15%), FTLD-ALS (65%) and ALS (40%). No curative treatment actually exists, but therapeutics emerged against tau aggregation. The objectives of the project are to develop appropriate cognitive, brain imaging markers and peripheral biomarkers of the early phase of FTLD, to follow disease progression and to guide future targeted therapeutic trials. To address this questions, we will conduct a multimodal study (cognition, brain structural MRI, brain metabolism - FDG-PET) in C9ORF72 families. The cohort will be followed at 3-time points (M0, M18, M36). Longitudinal analyses will aim at characterizing the trajectory of decline across time. Brain structural changes will be evaluated by 1) morphometric analysis to assess global brain atrophy, cortical thickness and study of the cortical sulci; 2) functional connectivity analysis of resting-state MR data; 3) structural connectivity analysis of diffusion-weighted MRI. Brain metabolism will be evaluated with FDG-PET. We will use the most recent RNA sequencing technology to detect gene expression and RNA splicing alterations in lymphocytes of patients and presymptomatic carriers. The discovery of new markers involved in FTLD will have practical consequences for early and accurate diagnosis of FLD and ALS disease.

9.1.2.5. ANR IVMRS

Participants: Anne Bertrand [Correspondant], Alexandra Petiet, Mathieu Santin, Francesca Branzoli, Benoit Delatour, Marc Sanson.

Project acronym: IVMRS

Project title: Implantable miniaturized probe for In-vivo Magnetic Resonance Spectroscopy: Application to Murine models of Alzheimer's disease and Gliomas.

Duration: Oct 2016 - Oct 2020

Amount: 633k€

Coordinator: Luc Hebrard

Other partners: ICube - Unistra, Strasbourg; ISA Laboratory, Lyon; NYU School of Medicine, NY, USA.

Abstract: During the development of new therapeutics against brain diseases, the pre-clinical phase, i.e. the validation of treatment delivery, safety and efficacy in animal models of the disease, represents a crucial step. Magnetic Resonance Imaging (MRI) is a method of particular interest at this stage, as it provides non-invasive surrogate endpoints that can help selecting appropriate candidates during the process of drug development. Single Voxel Magnetic Resonance Spectroscopy (SVS) provides non-invasive, in-vivo quantitative measurements of brain metabolites, which reflects functional changes at the cellular and subcellular levels, and can be repeated longitudinally. As high-field MRI has become the benchmark in preclinical research on animal models, it appears possible to investigate the cerebral metabolomics changes in animals, and to use it as a surrogate marker in preclinical therapeutic trials. However, the number of relevant metabolites is much higher than the low number of measurable metabolites with conventional in-vivo high-field SVS. Moreover, considering also the subtle changes of these metabolites at the early stage of the disease, the use of conventional high-field SVS in preclinical studies remains strongly limited. The high volume of the Voxel-of-Interest (VOI), ranging from 10 to 30mm3, which is required to have a usable signal in conventional SVS, and the inherent variability of longitudinal SVS measurement due to the variable position of the VOI in the successive experiments, remain the two major issues when looking during time for small changes in metabolic concentrations and metabolites ratios in a specific small region of the animal brain. The IvMRS project aims at filling this gap by developing the first chronic implantable MRS micro-probe, minimally invasive, exhibiting very high signal sensitivity, and sharp

spectral peaks, from sub-millimetric VOI. Such a probe will allow detecting a much higher number of metabolites than conventional in-vivo SVS. The probe will work at frequencies ranging from 300MHz to 500MHz in ultra-high field Magnetic Resonance Imaging scanners, 7T and 11.7T. It will embed a specific micro-coil antenna, a low-noise signal conditioning circuit designed in CMOS microelectronics technology, as well as an accurate on-chip positioning sensor. It will be dedicated to the study of changes in brain metabolite markers of two major diseases, Alzheimer's disease and cerebral gliomas, and to the assessment of effective therapeutic strategies.

9.1.3. Inria Project Labs

9.1.3.1. IPL Neuromarkers

Participants: Stanley Durrleman [Correspondant], Olivier Colliot [Correspondant], Fabrizio de Vico Fallani, Anne Bertrand, Stéphane Epelbaum.

Project acronym: Neuromarkers

Project title: Design of imaging biomarkers of neurodegenerative diseases for clinical trials and study of their genetic associations

Duration: 2017-2021

Coordinators: Stanley Durrleman and Olivier Colliot

Other partners: Inria GENSCALE, Inria BONSAI, Inria DYLISS, Inria XPOP, ICM, IHU/ICM iConics

Abstract: The Inria Project Lab Neuromarkers aims to develop new statistical and computational approaches to integrate multimodal imaging and omics data and to demonstrate their potential to identify early alterations and predict progression of neurodegenerative diseases. To tackle this challenge, the project brings together multidisciplinary expertise from Inria and ICM (Brain and Spine Institute) in the fields of statistical learning, brain imaging, bioinformatics, knowledge modeling, genomics and neurodegenerative diseases.

9.1.4. IHU

9.1.4.1. General program

Participants: Olivier Colliot, Stanley Durrleman, Didier Dormont, Ninon Burgos, Stéphane Epelbaum, Fabrizio de Vico Fallani.

Project acronym: IHU-A-ICM

Project title: Institute of Translational Neuroscience

Founded in 2011

General Director: Bertrand Fontaine

The IHU-A-ICM program was selected, in 2011, in a highly competitive national call for projects. A 10-year, 55M€ program, has been implemented by a recently created foundation for scientific cooperation. Based on the clinical and scientific strenghts of the ICM and the hospital Department of Nervous System Diseases, it mainly supports neuroscience research, but is also invested in improving care and teaching. ARAMIS is strongly involved in the IHU-A-ICM project, in particular in WP6 (neuroimaging and electrophysiology), WP7 (biostatistics), WP2 (Alzheimer) and WP5 (epilepsy). We have started collaborations with the new bioinformatics/biostatistics platform (IHU WP7, head: Ivan Moszer), in particular through a joint project on the integration of imaging and genomics data.

9.1.4.2. ICM-Internal Research projects

Participants: Anne Bertrand [Correspondant], Takoua Kaaouana, Benoit Delatour, Alexandra Petiet, Olivier Colliot, Arnaud Marcoux.

Project title: The Histo-MRI project: targeting MR signature of tauopathy from micro- to macroscopy

Started in 2014

Coordinator: Anne Bertrand

Identifying morphological MR signatures of brain diseases usually follows a top-down process, which starts by describing a pattern of MR signal changes in patients, hypothesizes an underlying pathological mechanism, and confirms this mechanism by correlating the observed MR signal changes with histological lesions on post-mortem examination. This top-down process, relevant for large, centimetric brain lesions, becomes inappropriate when targeting the MR signal intensity changes associated with microscopic lesions. Our project aims at developing an MR biomarker of NFT using a new bottom-up approach. We will start by identifying the MR signal changes associated with the presence of NFT at the level of the histological slice, and utilize these findings to develop a method of NFT quantification on clinical, millimetric 3D MR images. To achieve this goal, we will develop and implement a 11.7T histological coil dedicated to the scanning of histological slices, which allows both ultra-high resolution MR imaging (up to 33 microns in-plane) and perfect co-registration with histological staining, performed subsequently on the same slice. This method has the potential to provide a novel biomarker of tauopathy that could not have been identified using the usual top-down approach. It also envisions the possibility to describe and understand new MRI contrasts in other neurodegenerative diseases associated with microscopic deposition of various proteins.

9.1.4.3. ICM BBT Program - project PredictICD

Participants: Olivier Colliot [Correspondant], Jean-Christophe Corvol [Correspondant], Johann Faouzi.

Project title: Predict impulse control disorders in Parkinson's disease (PREDICT-ICD)

Started in 2018

Coordinators: Olivier Colliot and Jean-Christophe Corvol (ICM)

In Parkinson's disease (PD), the therapeutic strategy is based on the dopamine replacement therapy. Although available since the 1960s', it is only relatively recently that behavioral disorders associated with these drugs have been described. Gathered under the term of "behavioral addiction", they include impulse control disorders (ICDs), dopamine dysregulation syndrome (DDS), and punding. Interestingly, whereas addiction to L-dopa itself occurs quasi exclusively with L-dopa, ICDs appear electively under dopamine agonist (DA) therapy. The objectives of this project are: i) to elucidate the genetic basis of DA induced ICDs in PD patients from several international cohorts; ii) to develop and validate a machine learning model to predict the occurrence of ICDs from the combination of clinical and genetic data.

9.1.4.4. ICM BBT Program - project DYNAMO

Participants: Stanley Durrleman [Correspondant], Harald Hampel [Correspondant], Sabrina Fontanella, Simone Lista, Olivier Colliot, Stephanie Allassonniere, Jean-Baptiste Schiratti, Bruno Dubois, Hovagim Bakardjian, Remi Genthon, Enrica Cavedo, Katrine Rojkowa.

Project title: Dynamic models of disease progression across Alzheimer's disease stages informed by multimodal neuroimaging and biological data

Started in 2016

Coordinator: Stanley Durrleman and Harald Hampel

Other partners: Institut de la Mémoire et de la maladie d'Alzheimer

The estimation of data-driven models of disease progression for neurodegenerative diseases, including Alzheimer's disease (AD), is crucial to confirm, refine and extend the current hypothetical models. The estimation of such quantitative models from longitudinal data sets is notably difficult because of the lack of principled methodological frameworks for the analysis of spatiotemporal data.

The project builds on an innovative mathematical, statistical, and computational framework to automatically align the dynamics and the direction of individual trajectories of the evolving pathology, and then to infer a normative scenario of disease progression across different disease stages. The estimated scenario will combine spatiotemporal maps of lesion propagation, such as maps of amyloid deposition or cortical atrophy, and global measurements such as levels of CSF biomarkers. It will be possible to estimate not only a normative scenario but also the inter-individual variability in the values, dynamics and direction of both topographical and pathophysiological biomarkers changes during the course of the disease.

The application of this technology to publicly available and in-house longitudinal data sets of individuals from the asymptomatic at risk to the prodromal and dementia stages will yield new insights into the pathophysiology of AD from the preclinical to the AD dementia stages. This quantitative data-driven approach will be exploited to assess and refine the current qualitative hypothetical models of AD progression. Notably, it will complement these models with typical pathways of lesion propagation in the brain during disease progression. It will also highlight the effect of the known risk factors of AD such as apolipoprotein E genotype on the disease progression profile.

The project will open up the concrete possibility to derive a computer-aided diagnosis, staging, and prognosis tool for a better recruitment of patients in clinical studies and to assist clinicians in the diagnosis and the monitoring of both disease progression and treatment efficacy.

9.1.4.5. ICM BBT Program - project SEMAPHORE

Participants: Stanley Durrleman [Correspondant], Stéphane Lehéricy [Correspondant], Jean-Christophe Corvol, Marie Vidailhet, Raphael Couronné, Safia Said.

Project title: Personalized progression model of Parkinson's disease

Started in 2018

Coordinator: Stanley Durrleman and Stéphane Lehéricy

Other partners: Neurology and Neuro-radiology departments, Pitié-Salpêtrière Hospital, AP-HP

The aim of this project is to build a personalizable model of Parkinson's disease (PD) progression integrating the complex dynamical interplay between phenotypic, imaging, genetic and metabolic alterations. We will identify and validate markers for monitoring of progression of brain damage in early and prodromal PD and identify conversion markers in subjects at risk of PD (idiopathic rapid eye movement sleep behavior disorders iRBD, PD- related mutation carriers). We will describe the appearance, characterize clinical phenotypes of PD, and identify modifier genes of disease phenotype. To this aim, we will relie on a novel statistical learning method using Bayesian non-linear mixed-effects model allowing to combine and realign short term sequence data to estimate a long-term scenario of disease progression. This method is able to estimate individual stages of disease progression and to analyze automatically non-linear spatiotemporal patterns of data change. It estimates both a group-average scenario of PD progression as well as the inter-individual variability of this model in terms of age at onset, pace of disease progression and variability in the spatiotemporal trajectory of data changes. We will analyse the effect of genetic variants in the modulation of these non-linear progression patterns, and assess the statistical power of the individual parameters encoding for these patterns. The method will be applied to two sets of longitudinal data from the local prospective NUCLEIPARK (60 PD patients, 20 patients with iRBD, 60 controls) and ICEBERG studies (200 early idiopathic PD, 50 iRBD, 30 GBA and LRRK2 PD-related mutation carriers, 50 controls). Examinations included clinical, biological, and neurophysiological data, and multimodal 3T MRI, DATScan, and skin and salivary gland biopsies. The models of PD progression for each category of subjects will be released to the community, as well as the software for reproducibility purposes.

9.1.4.6. ICM BBT Program - project ATTACK

Participants: Fabrizio de Vico Fallani [Correspondant], Charlotte Rosso [Correspondant], Marie-Constance Corsi, Laurent Hugueville.

Project title: ATTACK Brain Network Models Of Motor Recovery After Stroke

Started in 2018

Coordinator: Fabrizio De Vico Fallani, Charlotte Rosso

Other partners: Neurology and Stroke departments, Pitié-Salpêtrière Hospital, AP-HP

Like in other connected systems, studying the structure of the interactions between different brain regions has profound implications in the comprehension of emergent complex phenomena as, for example, the capability of the human brain to functionally reorganize after cerebrovascular "attacks" or stroke. This dynamic skill, which is known in neuroscience as neural plasticity, is not only interesting from a network science perspective, but it also plays a crucial role in determining the motor/cognitive recovery of patients who survive a stroke. As a critical innovation, this project proposes to develop a systematic and rigorous approach based on neuroimaging techniques, signal processing, and network science for the modeling and analysis of temporally dynamic neural processes that characterize motor recovery after stroke. To achieve these goals, this project is organized around the following objectives: i) acquiring a comprehensive longitudinal dataset of brain and behavioral/clinical data after stroke, ii) developing new analytic tools to characterize and generate temporally dynamic brain networks, iii) building network-based models of motor recovery after stroke, accounting for individual patients. These objectives involve an intensive gathering of heterogeneous mass data, their processing, the subsequent outcome interpretation and statistical simulation, as well as the development of longitudinal models and network-based diagnostics of the patient's motor recovery progress. Results will be first characterized from pure network-theoretic and neuroscience perspectives, so as to highlight fundamental research challenges, and then validated to clarify the importance and the applicability to the clinical scenario. Our results will unveil multiscale properties of dynamic brain networks and identify predictive neuromarkers for motor recovery after stroke. This project has a two-fold impact on the society. On the one hand, it will provide new methods and robust tools to properly characterize and model temporally dynamic networks in neuroscience. On the other hand, it will provide longitudinal models of motor recovery in stroke patients that can potentially unveil the neural substrate that underpins rehabilitation, improve prognosis, and eventually lower cost of hospitalization time. From a broader perspective this interdisciplinary project proposes a transformative approach to analyze large-scale neural systems.

9.1.5. 3IA Institutes - PRAIRIE

Participants: Olivier Colliot, Stanley Durrleman, Ninon Burgos.

Project acronym: PRAIRIE

Project title: Paris Artificial Intelligence Research Institute

Founded in 2019

Director: Isabelle Ryl

Website: https://prairie-institute.fr/

PRAIRIE is one of the four selected French Institutes of AI. It was selected within a call for creation of interdisciplinary AI research institutes (or "3IAs" for "Instituts Interdisciplinaires d'Intelligence Artificielle"), as part of the national French initiative on Artificial Intelligence (AI). PRAIRIE aspires to become within five years a world leader in AI research and higher education, with an undeniable impact on economy and technology at the French, European and global levels. ARAMIS team members N. Burgos, O. Colliot and S. Durrleman hold a chair at PRAIRIE.

9.1.6. National Networks

- GdR Statistics and Medicine - http://gdr-stat-sante.math.cnrs.fr/spip/
- GdR (MaDICS) Masses de Données, Informations et Connaissances en Sciences Big Data - Data ScienceStatistics and Medicine - http://www.madics.fr/reseaux/
- F. De Vico Fallani participated to the GdR (HANDICAP) in the framework of the future strategy of Inria
- F. De Vico Fallani was founding member of the CORTICO national network for brain-computer interfaces

9.1.7. Other National Programs

9.1.7.1. Fondation Vaincre Alzheimer

Participants: Olivier Colliot, Vincent Henry, Martin Hoffman-Apitius.

Project title: Integrative multiscale knowledge model of Alzheimer's disease pathophysiology

2019-2020

Amount: 100K€

Coordinator: Olivier Colliot

Other partners: Frauhofer SCAI (Germany)

Abstract: Alzheimer's disease (AD) pathophysiology is still imperfectly understood. In particular, we currently lack an integrative view of the disease to interconnect knowledge about the molecular, cellular, clinical and systems levels that remain scattered. Computational knowledge models have the potential to provide such an integrative view. The aim of this project is to provide a multiscale knowledge model of AD pathophysiology by aggregating existing heterogeneous resources (disease maps, ontologies, databases) using Semantic Web standards. The resulting model and associated software tools will be made publicly available to the scientific community.

9.1.7.2. France Parkinson

Participants: Jean-Christophe Corvol, Olivier Colliot, Stanley Durrleman.

Project title: PRECISE-PD - From pathophysiology to precision medicine for Parkinson's disease

2019-2024

Amount: 3M€

Coordinator: Jean-Christophe Corvol

Other partners: Inserm CIC-1436, Inserm CIC-P1421, Inserm U1171, Université de Bordeaux (IMN), University of Glasgow, University of Calgary,

Abstract: Parkinson's disease (PD) is a complex neurodegenerative disease characterized by the progression of motor and non-motor symptoms resulting from the spreading of the disease into dopaminergic and non-dopaminergic areas. Clinical trials have failed to demonstrate efficacy to slow PD progression because the relationships between progression profiles and their underlying molecular mechanisms remain to be identified. The objective of PRECISE-PD is to propose a mechanismsbased progression model of PD by combining genetic and longitudinal clinical data from a large cohort of patients. We will implement a biobank to the NS-PARK/FCRIN cohort collecting motor and non-motor symptoms from >22,000 PD patients followed in the 24 expert centers in France. Genomic data will be generated by using a microarray platform developed for neurodegenerative diseases studies, and brain imaging will be obtained from a subgroup of patients. Computational and machine learning approaches will be developed to address the challenges of analyzing the high dimensionality and the mixture of data necessary to move beyond empirical stratification of patients. Replication will be performed in independent cohorts, and biological validation will combine biomarkers and preclinical research. PRECISE-PD is an unpreceded opportunity to open the path to the new era of precision and personalized medicine for PD.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. H2020 - Project EuroPOND

Participants: Olivier Colliot, Stanley Durrleman, Manon Ansart, Igor Koval, Alexandre Bône.

Project acronym: EuroPOND

Project title: Data-driven models for Progression Of Neurological Disease

Duration: Jan 2016 - Dec 2019

Amount: 6M€

Coordinator: Daniel Alexander

Other partners: University College London (UK), EMC Rotterdam (The Netherlands), VUMC (The Netherlands), Fate Bene Fratelli (Italy), Carol Besta Institute (Italy), Université de Genève (Switzerland), Icometrix (Belgium)

Abstract: EuroPOND will develop a data-driven statistical and computational modeling framework for neurological disease progression. This will enable major advances in differential and personalized diagnosis, prognosis, monitoring, and treatment and care decisions, positioning Europe as world leaders in one of the biggest societal challenges of 21st century healthcare. The inherent complexity of neurological disease, the overlap of symptoms and pathologies, and the high comorbidity rate suggests a systems medicine approach, which matches the specific challenge of this call. We take a uniquely holistic approach that, in the spirit of systems medicine, integrates a variety of clinical and biomedical research data including risk factors, biomarkers, and interactions. Our consortium has a multidisciplinary balance of essential expertise in mathematical/statistical/computational modelling; clinical, biomedical and epidemiological expertise; and access to a diverse range of datasets for sporadic and well-phenotyped disease types.The project will devise and implement, as open-source software tools, advanced statistical and computational techniques for reconstructing long-term temporal evolution of disease markers from cross-sectional or short-term longitudinal data. We will apply the techniques to generate new and uniquely detailed pictures of a range of important diseases. This will support the development of new evidence-based treatments in Europe through deeper disease understanding, better patient stratification for clinical trials, and improved accuracy of diagnosis and prognosis. For example, Alzheimer's disease alone costs European citizens around €200B every year in care and loss of productivity. No disease modifying treatments are yet available. Clinical trials repeatedly fail because disease heterogeneity prevents bulk response. Our models enable fine stratification into phenotypes enabling more focussed analysis to identify subgroups that respond to putative treatments.

9.2.1.2. H2020 - Project VirtualBrainCloud

Participant: Stanley Durrleman.

Project acronym: TVBCloud

Project title: Personalized Recommendations for Neurodegenerative Disease

Duration: Jan 2019 - Dec 2022

Amount: 15 M€

Coordinator: Petra Ritter

Other partners: Charite Berlin, Université Aix Marseille, Fraunhofer Gesellschaft, University of Oxford, Forschungzentrum Juelich, Institut du Cerveau et de la Moëlle épinière, Inria, Fundacio institut de bioenginyeria de catalunya, Helsingin yliopisto, Universita degli studi di genova, Universidad complutense de Madrid, Codebox Computer-Dienste, Codemart, Eodyne Systems, Universität Wien, TP21, Alzheimer Europe

Abstract: The annual worldwide cost of Alzheimer's dementia was 777.81 billion Euro in 2015. This number will rise to 7.41 trillion Euro in 2050. Early diagnosis would save up to $7.9 trillion in medical and care costs by 2050 in the US alone. However, the emergent pathology is highly variable across people, necehighly variable across people, necessitating individualized diagnostics and interventions. The VirtualBrainCloud addresses this by bridging the gap between computational neuroscience and subcellular systems biology, integrating both research streams into a unifying computational model that supports personalized diagnostics and treatments in NDD. TheVirtualBrainCloud not only integrates existing software tools, it also merges the efforts of two big EU initiatives, namely The Virtual Brain large scale simulation platform of the EU Flagship Human Brain Project and IMI-EPAD initiative (European prevention of Alzheimer's dementia consortium). VirtualBrainCloud will develop and validate a decision support system that provides access to high quality multi-disciplinary data for clinical practice. The result will be a cloud-based brain simulation platform to support personalized diagnostics and treatments in NDD. The EU PRACE (Partnership for Advanced Computing in Europe) initiative, will provide the required computing infrastructure. TheVirtualBrainCloud will develop robust solutions for legal and ethical matters by interacting with EU projects such as European Open Science Cloud (EOSC), 'cloud4health', Alzheimer's Europe patient organizations and ELIXIR, an organization that manages and safeguards EU research data. Our software developers have already produced highly successful brain simulation and clinical decision support tools. The resulting software will be a cloud based computational modeling system that is tailored to the individual, and bridges multiple scales to identify key mechanisms that predict NDD progression and serves as Precision Decision Support System.

9.2.1.3. FET Flagship - Human Brain Project

Participants: Olivier Colliot, Stanley Durrleman.

Project acronym: HBP

Project title: Human Brain Project

Sub-project: SP8 - Medical Informatics Platform

Duration: 2016-

Abstract: The Human Brain Project (HBP) is a European Commission Future and Emerging Technologies Flagship. The HBP aims to put in place a cutting-edge, ICT-based scientific Research Infrastructure for brain research, cognitive neuroscience and brain-inspired computing. The Project promotes collaboration across the globe, and is committed to driving forward European industry. Our team is involved in the Subproject SP8 (Medical Informatics Platform). The Medical Informatics Platform (MIP) is an innovative data management system that gives researchers the means to access and analyse large amounts of anonymized clinical neuroscience data. Within that framework, we will develop and implement a method to construct disease progression models from longitudinal biomarkers. The method will use statistical learning techniques to infer a long-term disease progression model from multiple short term data from a series of individuals. The model will account for variability in age at disease onset, pace of disease progression and trajectories of biomarkers changes across individuals in the observed population.

9.2.1.4. ERC - LEASP

Participant: Stanley Durrleman.

Project acronym: LEASP

Project title: Learning Spatiotemporal Patterns in Longitudinal Image Data Sets of the Aging Brain

Duration: 2016-2021

Abstract: Time-series of multimodal medical images offer a unique opportunity to track anatomical and functional alterations of the brain in aging individuals. A collection of such time series for several individuals forms a longitudinal data set, each data being a rich iconic-geometric representation of the brain anatomy and function. These data are already extraordinary complex and variable across individuals. Taking the temporal component into account further adds difficulty, in that each individual follows a different trajectory of changes, and at a different pace. Furthermore, a disease is here a progressive departure from an otherwise normal scenario of aging, so that one could not think of normal and pathologic brain aging as distinct categories, as in the standard case-control paradigm.

Bio-statisticians lack a suitable methodological framework to exhibit from these data the typical trajectories and dynamics of brain alterations, and the effects of a disease on these trajectories, thus limiting the investigation of essential clinical questions. To change this situation, we propose to construct virtual dynamical models of brain aging by learning typical spatiotemporal patterns of alterations propagation from longitudinal iconic-geometric data sets.

By including concepts of the Riemannian geometry into Bayesian mixed effect models, the project will introduce general principles to average complex individual trajectories of iconic-geometric changes and align the pace at which these trajectories are followed. It will estimate a set of elementary spatiotemporal patterns, which combine to yield a personal aging scenario for each individual. Disease-specific patterns will be detected with an increasing likelihood.

This new generation of statistical and computational tools will unveil clusters of patients sharing similar lesion propagation profiles, paving the way to design more specific treatments, and care patients when treatments have the highest chance of success.

9.3. International Initiatives

9.3.1. Informal International Partners

- O. Colliot has an enduring collaboration with the Center for Magnetic Resonance Research, University of Minnesota, USA (P-F Van de Moortele, T. Henry).
- S. Durrleman and O. Colliot have a collaboration with the Center for Medical Image Computing (CMIC) at University College London (UCL), London, UK (D. Alexander, H. Zhang).
- F. De Vico Fallani has a collaboration with Penn University, US (Prof. D. Bassett) and Queen Mary University London, UK (Prof. Vito Latora).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

We hosted Prof Bruno Jedynak from Portland State University (USA) in June and July 2019.

CAGE Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- ANR SRGI, for *Sub-Riemannian Geometry and Interactions*, coordinated by **Emmanuel Trélat**, started in 2015 and runs until 2020. Other partners: Toulon University and Grenoble University. SRGI deals with sub-Riemannian geometry, hypoelliptic diffusion and geometric control.
- ANR Finite4SoS, for *Commande et estimation en temps fini pour les Systèmes de Systèmes*, coordinated by Wilfrid Perruquetti, started in 2015 and run up to this year. Other partners: Inria Lille, CAOR - ARMINES. Finite4SoS aims at developing a new promising framework to address control and estimation issues of Systems of Systems subject to model diversity, while achieving robustness as well as severe time response constraints.
- ANR QUACO, for *QUAntum COntrol: PDE systems and MRI applications*, coordinated by Thomas Chambrion, started in 2017 and runs until 2021. Other partners: Lorraine University. QUACO aims at contributing to quantum control theory in two directions: improving the comprehension of the dynamical properties of controlled quantum systems in infinite-dimensional state spaces, and improve the efficiency of control algorithms for MRI.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Program: H2020-EU.1.3.1. - Fostering new skills by means of excellent initial training of researchers

Call for proposal: MSCA-ITN-2017 - Innovative Training Networks

Project acronym: QUSCO

Project title: Quantum-enhanced Sensing via Quantum Control

Duration: From November 2017 to October 2021.

Coordinator: Christiane Koch

Coordinator for the participant Inria: Ugo Boscain

Abstract: Quantum technologies aim to exploit quantum coherence and entanglement, the two essential elements of quantum physics. Successful implementation of quantum technologies faces the challenge to preserve the relevant nonclassical features at the level of device operation. It is thus deeply linked to the ability to control open quantum systems. The currently closest to market quantum technologies are quantum communication and quantum sensing. The latter holds the promise of reaching unprecedented sensitivity, with the potential to revolutionize medical imaging or structure determination in biology or the controlled construction of novel quantum materials. Quantum control manipulates dynamical processes at the atomic or molecular scale by means of specially tailored external electromagnetic fields. The purpose of QuSCo is to demonstrate the enabling capability of quantum control for quantum sensing and quantum measurement, advancing this field by systematic use of quantum control methods. QuSCo will establish quantum control as a vital part for progress in quantum technologies. QuSCo will expose its students, at the same time, to fundamental questions of quantum mechanics and practical issues of specific applications. Albeit challenging, this reflects our view of the best possible training that the field of quantum technologies can offer. Training in scientific skills is based on the demonstrated tradition of excellence in research of the consortium. It will be complemented by training in communication and commercialization. The latter builds on strong industry participation whereas the former existing expertise on visualization and gamification and combines it with more traditional means of outreach to realize target audience specific public engagement strategies.

8.3. International Research Visitors

8.3.1. Internships

Rosa Kowalewski made an internship under the supervision of Barbara Gris from January to May 2019.

CAMBIUM Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR projects

8.1.1.1. 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.

In 2019, progress was made on the definition of Gospel, a standard language for annotating OCaml programs with logical specifications, which could be understood and processed by several verification tools, including Why3 and CFML.

8.2. International Research Visitors

8.2.1. Visits of International Scientists

Jacques Garrigue (Nagoya University) is staying with our team in Paris from September 2019 to June 2020. He has long been one of the key designers and implementors of the OCaml type system. We are collaborating on the design of new language features and on a possible re-design of the type-checker implementation.

CASCADE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives with Industry

7.1.1. ANBLIC: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – December 2020

Coordinator: Wallix

Partners: UPEC, CEA, 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.

7.1.2. RISQ: Regroupement de l'Industrie française pour la Sécurité Post-Quantique

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 and Phong Nguyen since September 2019

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: 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: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – December 2019

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. SaFED: Safe and Functional Encrypted Databases

Program: ANR JCJC

Duration: October 2019 – Septembre 2023

PI: Brice Minaud

Partners: ENS, DGA

This project addresses the security of encrypted databases, with the proposal of new searchable encryption techniques and deeper security analysis.

7.2.4. ALAMBIC: 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. CryptoCloud: 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.

7.3.2. SAFEcrypto: 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.

7.3.3. ECRYPT-NET: 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.

7.3.4. aSCEND: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2021

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.

7.3.5. FENTEC: 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: 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

7.5.1. Professors

- Sep 1 - Oct 31, 2019: Manuel Barbosa (University of Porto)
- Jun 20 - 21, 2019: Jean Paul Degabriele (TU Darmstadt)
- Jun 20 - 30, 2019: Joël Alwen (Wickr)
- Jul 4-5, 2019: David Wu (University of Virginia)

7.5.2. PhD students

- Jun 18 - 25, 2019: Ward Beullens (KU Leuven)
- Jun 15 - Jul 1, 2019: Rotem Tsabary (Weizmann)
- June 1 - 30, 2019: Hendrik Waldner (Edinburgh)
- Jun 23 - Jul 3, 2019: Naty Peter (Ben-Gurion University)

7.6. Internships

- Apr-Sep 2019: Hugo Marival (Ecole Polytechnique) - Michel Abdalla and David Pointcheval
- Apr-Sep 2019: Thibaut Bagory (ENS Paris-Saclay - UVSQ) - Brice Minaud
- Oct-Dec 2019: Marie Euler (X - DGA) - Brice Minaud

COML Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Collaboration with the Willow Team:

- co-advising with J. Sivic and I. Laptev of a PhD student: Ronan Riochet.
- construction of a naive physics benchmark (http://www.intphys.com)

Collaboration with the Almanach Team:

- co-advising with B. Sagot a PhD student: Robin Algayres.
- co-advising with B. Sagot a Master student: Charlotte Rochereau

8.2. National Initiatives

8.2.1. ANR

- **ANR-Transatlantic Platform Digging into Data - ACLEW** (2017–2020. 5 countries; Total budget: 1.4M€; coordinating PI : M. Soderstrom; Local PI: A. Cristia; Leader of tools development and co-PI : E. Dupoux) - Constructing tools for the Analysis of Children's Language Experiences Around the World.
- **CNRS Prematuration - BabyCloud**. (2018-2019; coordinating PIs : E. Dupoux and X.-N. Cao; 100€) - Enable the construction of a fully functionnal Baby Logger prototype; perform a market analysis and prepare the launch of a startup.
- **ANR GEOMPHON**. (2018-2021; coordinating PI : E. Dunbar; 299K€) - Study the effects of typologically common properties of linguistic sound systems on speech perception, human learning, and machine learning applied to speech.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

- Johns Hopkins University, Baltimore, USA: S. Kudanpur, H. Hermanksy
- RIKEN Institute, Tokyo, Japan: R. Mazuka

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Justine Cassell (CMU, ARP, PRAIRIE Chair starting from Oct 2019)

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

+ E. Dupoux, Research Scientist, JSALT Workshop, Montreal (July, 2019)

COMMEDIA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. ANR Project "IFSMACS"

Participants: Muriel Boulakia, Céline Grandmont [local coordinator].

Period: 2015-2019.
The objective of this project, coordinated by Takéo Takahashi (Inria Nancy Grand-Est), is the mathematical analysis of systems involving structures immersed in a fluid. This includes the asymptotic analysis, the study of the controllability and stabilization of fluid-structure interaction systems, the understanding of the motion of self-propelled structures and the analysis and development of numerical methods to simulate fluid-structure systems.

9.1.1.2. ANR Project "ADAPT"

Participants: Maria Fuente-Ruiz, Damiano Lombardi [coordinator], Olga Mula.

Period: 2018-2022.
Adaptive Dynamical Approximations by Parallel Tensor methods. The main goal of the ANR is to investigate the numerical approximation of the solution of high-dimensional problems. In particular, the applications that motivate this study are the Uncertainty Quantification and the Kinetic theory. The main objective is to construct in an adaptive way parsimonious discretisations starting from arbitrarily chosen separated discretisations.

DELYS Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. AdeCoDS (2019–2023)

Title: Programming, verifying, and synthesizing Adequately-Consistent Distributed Systems (AdeCoDS).

Members: Université de Paris (project leader), Sorbonne-Université LIP6, ARM, Orange.

Funding: The total funding of AdeCoDS from ANR is 523 471 euros, of which 162 500 euros for Delys.

Objectives The goal of the project is to provide a framework for programming distributed systems that are both correct and efficient (available and performant). The idea is to offer to developers a programming framework where it is possible, for a given application, (1) to build implementations that are correct under specific assumptions on the consistency level guaranteed by the infrastructure (e.g., databases and libraries of data structures), and (2) to discover in a systematic way the different trade-offs between the consistency level guaranteed by the infrastructure and the type and the amount of synchronization they need to use in their implementation in order ensure its correctness. For that, the project will develop a methodology based on combining (1) automated verification and synthesis methods, (2) language-based methods for correct programming, and (3) techniques for efficient system design.

7.1.1.2. ESTATE - (2016–2021)

Members: LIP6 (DELYS, project leader), LaBRI (Univ. de Bordeaux); Verimag (Univ. de Grenoble).

Funding: ESTATE is funded by ANR (PRC) for a total of about 544 000 euros, of which 233 376 euros for DELYS.

Objectives: The core of ESTATE consists in laying the foundations of a new algorithmic framework for enabling Autonomic Computing in distributed and highly dynamic systems and networks. We plan to design a model that includes the minimal algorithmic basis allowing the emergence of dynamic distributed systems with self-* capabilities, *e.g.*, self-organization, self-healing, self-configuration, self-management, self-optimization, self-adaptiveness, or self-repair. In order to do this, we consider three main research streams:

(i) building the theoretical foundations of autonomic computing in dynamic systems, (ii) enhancing the safety in some cases by establishing the minimum requirements in terms of amount or type of dynamics to allow some strong safety guarantees, (iii) providing additional formal guarantees by proposing a general framework based on the Coq proof assistant to (semi-)automatically construct certified proofs.

The coordinator of ESTATE is Franck Petit.

7.1.1.3. RainbowFS - (2016–2020)

Members: LIP6 (DELYS, project leader), Scality SA, CNRS-LIG, Télécom Sud-Paris, Université Savoie-Mont-Blanc.

Funding: is funded by ANR (PRC) for a total of 919 534 euros, of which 359 554 euros for DELYS.

Objectives: RainbowFS proposes a "just-right" approach to storage and consistency, for developing distributed, cloud-scale applications. Existing approaches shoehorn the application design to some predefined consistency model, but no single model is appropriate for all uses. Instead, we propose tools to co-design the application and its consistency protocol. Our approach reconciles the conflicting requirements of availability and performance vs. safety: common-case operations are designed to be asynchronous; synchronisation is used only when strictly necessary to satisfy the application's integrity invariants. Furthermore, we deconstruct classical consistency models into orthogonal primitives that the developer can compose efficiently, and provide a number of tools for quick, efficient and correct cloud-scale deployment and execution. Using this methodology, we will develop an entreprise-grade, highly-scalable file system, exploring the rainbow of possible semantics, and we demonstrate it in a massive experiment.

The coordinator of RainbowFS is Marc Shapiro.

7.1.2. LABEX

7.1.2.1. SMART - (2012–2019)

Members: ISIR (Sorbonne Univ./CNRS), LIP6 (Sorbonne Univ./CNRS), LIB (Sorbonne Univ./INSERM), LJLL (Sorbonne Univ./CNRS), LTCI (Institut Mines-Télécom/CNRS), CHArt-LUTIN (Univ. Paris 8/EPHE), L2E (Sorbonne Univ.), STMS (IRCAM/CNRS).

Funding: Sorbonne Universités, ANR.

Description: The SMART Labex project aims globally to enhancing the quality of life in our digital societies by building the foundational bases for facilitating the inclusion of intelligent artifacts in our daily life for service and assistance. The project addresses underlying scientific questions raised by the development of Human-centered digital systems and artifacts in a comprehensive way. The research program is organized along five axes and DELYS is responsible of the axe "Autonomic Distributed Environments for Mobility."

The project involves a PhD grant of 100 000 euros over 3 years.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. LightKone

Title: Lightweight Computation for Networks at the Edge

Programm: H2020-ICT-2016-2017

Duration: January 2017 - December 2019

Coordinator: Université Catholique de Louvain

Partners:

Université Catholique de Louvain (Belgium)

Technische Universitaet Kaiserslautern (Germany)

INESC TEC - Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciencia (Portugal)

Faculdade de Ciencias E Tecnologiada Universidade Nova de Lisboa (Portugal)

Universitat Politecnica De Catalunya (Spain)

Scality (France)

Gluk Advice B.V. (Netherlands)

Inria contact: Marc Shapiro

The goal of LightKone is to develop a scientifically sound and industrially validated model for doing general-purpose computation on edge networks. An edge network consists of a large set of heterogeneous, loosely coupled computing nodes situated at the logical extreme of a network. Common examples are networks of Internet of Things, mobile devices, personal computers, and points of presence including Mobile Edge Computing. Internet applications are increasingly running on edge networks, to reduce latency, increase scalability, resilience, and security, and permit local decision making. However, today's state of the art, the gossip and peer-to-peer models, give no solution for defining general-purpose computations on edge networks, i.e., computation with shared mutable state. LightKone will solve this problem by combining two recent advances in distributed computing, namely synchronisation-free programming and hybrid gossip algorithms, both of which are successfully used separately in industry. Together, they are a natural combination for edge computing. We will cover edge networks both with and without data center nodes, and applications focused on collaboration, computation, and both. Project results will be new programming models and algorithms that advance scientific understanding, implemented in new industrial applications and a startup company, and evaluated in large-scale realistic settings.

7.3. International Initiatives

7.3.1. Participation in Other International Programs

7.3.1.1. Spanish research ministry project

Title: BFT-DYNASTIE - Byzantine Fault Tolerance: Dynamic Adaptive Services for Partitionable Systems

French Partners: Labri, Irisa, LIP6

International Partners (Institution - Laboratory - Researcher):

University of the Basque Country UPV - Spain, EPFL - LSD - Switzerland, Friedrich-Alexander-Universitat Erlangen-Nurenberg - Deutschland, University of Sydney - Australia

Duration: 2017–2019

The project BFT-DYNASTIE is aimed at extending the model based on the alternation of periods of stable and unstable behavior to all aspects of fault-tolerant distributed systems, including synchrony models, process and communication channel failure models, system membership, node mobility, and network partitioning. The two main and new challenges of this project are: the consideration of the most general and complex to address failure model, known as Byzantine, arbitrary or malicious, which requires qualified majorities and the use of techniques form the security area; and the operation of the system in partitioned mode, which requires adequate reconciliation mechanisms when two partitions merge.

7.3.1.2. Spanish research ministry project

Title: BFT-DYNASTIE - Byzantine Fault Tolerance: Dynamic Adaptive Services for Partitionable Systems

French Partners: Labri, Irisa, LIP6

International Partners (Institution - Laboratory - Researcher):

University of the Basque Country UPV - Spain, EPFL - LSD - Switzerland, Friedrich-Alexander-Universitat Erlangen-Nurenberg - Deutschland, University of Sydney - Australia

Duration: 2017–2019

The project BFT-DYNASTIE is aimed at extending the model based on the alternation of periods of stable and unstable behavior to all aspects of fault-tolerant distributed systems, including synchrony models, process and communication channel failure models, system membership, node mobility, and network partitioning. The two main and new challenges of this project are: the consideration of the most general and complex to address failure model, known as Byzantine, arbitrary or malicious, which requires qualified majorities and the use of techniques form the security area; and the operation of the system in partitioned mode, which requires adequate reconciliation mechanisms when two partitions merge.

7.3.1.3. STIC Amsud

Title: ADMITS - Architecting Distributed Monitoring and Analytics for IoT in Disaster Scenarios

International Partners (Institution - Laboratory - Researcher):

Universidad Diego Portales and Universidad Tecnica Federico Santa Maria (Chile)

Universidade Federal de Uberlandia, Universidade Federal do Rio Grande do Norte and Instituto Federal Sul-Rio-Grandense (Brazil)

Universidad de la Republica (Uuruguay)

Duration: 2019 - 2020

Start year: 2019

Develop algorithms, protocols and architectures to enable a decentralized distributed computing environment to provide support for failure monitoring and data analytics in Internet-of-Things (IoT) disaster scenarios.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

- AMOZARRAIN Ugaitz, PhD Student, University of San Sebastian (Spain), Feb. 2019 - Mar. 2019
- CORREA Leonardo, PhD Student, Federal University of Rio Grande do Sul (Brazil), Jan 2019 - Oct. 2019
- GOUVEIA LIMA Luan Teylo, PhD Student, UFF (Brazil), Sep. 2019-Mar. 2020
- PELC Andrzej, Professor, Université du Québec en Outaouais (Canada), Sep. 2019 - Oct. 2019
- DIEUDONNE Yoann, Associate Professor, Amiens Univ., Sep. 2019-Oct. 2019
- LONG Darrell, Professor, Univ. California Santa Cruz (USA), Feb. 2019 - Mar. 2019
- PARIS Jehan-François, Professor, University of Houston (USA), Feb. 2019 - Mar. 2019

7.4.2. Visits to International Teams

Marc Shapiro spent three weeks visiting Technical University Kaiserslautern during the Spring.

Luciana Arantes and Pierre Sens have been invited for 10 days at New-York University Shanghai

Luciana Arantes visited the network team at Pontifical Catholic University of Rio de Janeiro - PUC (Brazil)

Luciana Arantes and Pierre Sens visited the computer science department at Universidade Federal Fluminense - UFF (Brazl)

DYOGENE Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Laboratory of Information, Networking and Communication Sciences (LINCS)

Dyogene participates in LINCS https://www.lincs.fr, a research centre co-founded by Inria, Institut Mines-Télécom, UPMC and Alcatel-Lucent Bell Labs (currently Nokia Bell Labs) dedicated to research and innovation in the domains of future information and communication networks, systems and services.

9.1.2. PGMO

Dyogene participates in the PGMO (Gaspard Monge Program for Optimization, operations research, and their interactions with data science) via the project a 2 year project "Distributed control of flexible loads" funded through the ICODE/IROE call. This is a collaborative project between University Paris-Sud (PI: Gilles Stoltz) and Inria (PI: Ana Busic).

9.2. National Initiatives

9.2.1. GdR GeoSto

Members of Dyogene participate in Research Group GeoSto (Groupement de recherche, GdR 3477) http://gdr-geostoch.math.cnrs.fr/ on Stochastic Geometry led by and David Coupier [Université de Valenciennes].

This is a collaboration framework for all French research teams working in the domain of spatial stochastic modeling, both on theory development and in applications.

9.2.2. GdR RO

Members of Dyogene participate in GdR-RO (Recherche Opérationelle; GdR CNRS 3002), http://gdrro.lip6.fr/, working group COSMOS (Stochastic optimization and control, modeling and simulation), lead by A. Busic and E. Hyon (LIP 6); http://gdrro.lip6.fr/?q=node/78

9.2.3. ANR JCJC PARI

Probabilistic Approach for Renewable Energy Integration: Virtual Storage from Flexible Loads. The project started in January 2017. PI — A. Bušić. This project is motivated by current and projected needs of a power grid with significant renewable energy integration. Renewable energy sources such as wind and solar have a high degree of unpredictability and time variation, which makes balancing demand and supply challenging. There is an increased need for ancillary services to smooth the volatility of renewable power. In the absence of large, expensive batteries, we may have to increase our inventory of responsive fossil-fuel generators, negating the environmental benefits of renewable energy. The proposed approach addresses this challenge by harnessing the inherent flexibility in demand of many types of loads. The objective of the project is to develop decentralized control for automated demand dispatch, that can be used by grid operators as ancillary service to regulate demand-supply balance at low cost. We call the resource obtained from these techniques virtual energy storage (VES). Our goal is to create the necessary ancillary services for the grid that are environmentally friendly, that have low cost and that do not impact the quality of service (QoS) for the consumers. Besides respecting the needs of the loads, the aim of the project is to design local control solutions that require minimal communications from the loads to the centralized entity. This is possible through a systems architecture that includes the following elements: i) local control at each load based on local measurements combined with a grid-level signal; ii) frequency decomposition of the regulation signal based on QoS and physical constraints for each class of loads.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. NEMO

NEMO, NEtwork MOtion https://cordis.europa.eu/project/id/788851, https://project.inria.fr/ercnemo is an ERC Advanced Grant (2019 – 2024, PI François Baccelli). It is an inter-disciplinary proposal centered on network dynamics. The inter-disciplinarity spans from communication engineering to mathematics, with an innovative interplay between the two. NEMO's aim is to introduce dynamics in stochastic geometry. General mathematical tools combining stochastic geometry, random graph theory, and the theory of dynamical systems will be developed. NEMO will leverage interactions of Inria with Ecole Normale Supérieure on the mathematical side, and with Nokia Bell Labs and Orange on the engineering side. In March 2019, an inaugural workshop *Processus ponctuels et graphes aléatoires unimodulaires*https://project.inria.fr/ercnemo/fr/presentation was organized at Inria Paris.

9.3.2. Collaborations with Major European Organizations

Partner: VITO (Belgium); https://vito.be/en.

Co-advising of PhD student I. Shilov. Started: Nov 2019. Topic: "Algorithmic Games and Distributed Learning for Peer-to-Peer Energy Trading". PhD scholarship by VITO.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

- University of Florida; Collaborations with Prof Sean Meyn (ECE), Associate Prof Prabir Barooah (MAE), and the PhD students: A. Devraj (ECE), A. Coffman (MAE), N. Cammardella (ECE), J. Mathias (ECE).
- Sharif University, Tehran; Collaborations with O. Mirsadeghi.
- UC Berkeley; Collaborations with V. Anantharam.
- Indian Statistical Institute (ISI), Bangalore; Collaborations with Yogeshwaran D.

9.4.2. Participation in Other International Programs

9.4.2.1. Indo-French Center of Applied Mathematics

IFCAM Project "Geometric statistics of stationary point processes" B. Błaszczyszyn and Yogeshwaran D. from Indian Statistical Institute (ISI), Bangalore, have got in 2018 the approval from Indo-French Centre for Applied Mathematics (IFCAM), for their joint project on "Geometric statistics of stationary point processes" for the period 2018–2021. Yogeshwaran D. was visiting Dyogene for two weeks in March and November 2019.

9.4.2.2. Microsoft Research-Inria collaboration

Microsoft Research-Inria collaboration: Laurent Massoulié heads the Microsoft Research-Inria Joint Centre, and also participates to the "Distributed Machine Learning" project of the Joint Centre, together with Francis Bach (Inria), Sébastien Bubeck and Lin Xiao (MSR Redmond), and PhD student Hadrien Hendrikx.

9.4.2.3. Inria International Chairs

IIC- MEYN Sean

Title: Distributed Control and Smart Grid

International Partner (Institution - Laboratory - Researcher):

University of Florida (United States) - Department of Electrical and Computer Engineering - Sean Meyn

Duration: 2019 – 2023

Start year: 2019

See also: https://www.inria.fr/sites/default/files/2019-12/HoldersChairesInt_EN.pdf

TOPIC: “Distributed Control and Smart Grid”

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- Ali Khezeli [School of Mathematical Sciences, Tehran, Iran],
- Christian Hirsch [Bernoulli Institute, University of Groningen,
- David Métivier [Los Alamos National Laboratory, USA]
- Deepjyoti Deka [Los Alamos National Laboratory, USA]
- Guenter Last [Karlsruhe Institute of Technology, Germany],
- Hermann Thorisson [University of Islande],
- Holger Keeler [University of Melbourne, Australia] ,
- Hrvoje Pandžić [University of Zagreb, Croatia]
- Itai Benjamini [Weizmann Institute of Science, Rehovot, Israel],
- Joe Yukich [Lehigh University, Bethelem, PA, USA],
- Josu Doncel [University of the Basque Country, Spain],
- Lucas Pereira [Técnico Lisboa, Portugal]
- Miklós Abért [MTA Renyi Institute, Budapest, Hungary],
- Mir-Omid Haji-Mirsadeghi [Sharif University, Tehran, Iran],
- Natasa Dragovic [The University of Texas at Austin, TX, USA],
- Nelson Antunes [University of Faro, Portugal],
- Venkatachalam Anantharam [University of California, Berkeley, CA USA],
- Yogeshwaran D. [ISI, Bangalore, India],

9.5.1.1. Internships

- Bastien Dubail [École Normale Supérieure de Lyon],
- Emmanuel Kravitzch [Inria],
- Erwan Pichon [Inria].
- Ge Jin [Inria],
- Maxence Lefort [Inria].

9.5.2. Visits to International Teams

- C. Fricker: University of Faro, Portugal (one week).

9.5.2.1. Research Stays Abroad

- A.Busic: program participant (5 weeks in total) of “The mathematics of energy systems”, Isaac Newton Institute for Mathematical Sciences, Cambridge, UK. Spring 2019, https://www.newton.ac.uk/event/mes

EVA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. Inria Project Labs, Exploratory Research Actions and Technological Development Actions

- IPL SPARTA
- ATT SmartMarina, 2019. Help transfer the technology of the SmartMarina project to startup Falco. Keoma Brun-Laguna is lead.
- ADT 6TiSCH, 2018-2020. Benchmark the performance of 6TiSCH under realistic scenarios, through experimentaion using the OpenTestbed. Tengfei Chang is lead.
- ADT DASMU (Distributed Adaptive Scheduling for MUltichannel Wireless Sensor Networks), 2018-2019. DASMU focuses on a distributed scheduling algorithm which relies on realistic assumptions, does not require complex computation, is valid for any traffic load, is adaptive and compliant with the standardized protocols used in the 6TiSCH working group at IETF. First results have been obtained and an intensive simulation campaign made with the 6TiSCH simulator has provided comparative performance results. Our proposal, called YSF, outperforms MSF, the 6TiSCH Minimal Scheduling Function, in terms of end-to-end latency and end-to-end packet delivery ratio. Thanks to this ADT, Yasuyuki Tanaka has joined the EVA team for two years.

9.1.2. ANR

- The GeoBot FUI project (https://geobot.fr/) is one of the most innovative, challenging and fun projects around wireless localization in the world today. It applies true innovation to a real-world problem, with a clear target application (and customer) in mind. The GeoBot partners are building a small robot (think of a matchbox-sized RC car) that will be inserted into a gas pipe, and move around it to map the location of the different underground pipes. Such mapping is necessary to prevent gas-related accidents, for example during construction. At the end of the project, this solution will be commercialized and used to map the network of gas pipe in France, before being used in worldwide. Each partner is in charge of a different aspect of the problem: robotics, analysis of the inertial data, visualization, etc. Inria is in charge of the wireless part. We will be equipping the robot with a wireless chip(set) in order to (1) communicate with the robot as it moves about in the pipes while standing on the surface, and (2) discover the relative location of the robot w.r.t. a person on the surface. Inria is evaluating different wireless technologies, benchmarking around ranging accuracy and capabilities to communicate. We start from off-the-shelf kits from different vendors and build a custom board, benchmark it, and integrate it with the other partners of the project.

9.1.3. Other collaborations

- EVA has a collaboration with Orange Labs. **Thomas Watteyne** supervises the PhD of Mina Rady, which happens under a CIFRE agreement with Orange Labs.
- EVA has a collaboration with Vedecom. **Paul Muhlethaler** supervises Fouzi Boukhalfa's PhD funded by Vedecom. This PhD aims at studying low latency and high reliability vehicle-to-vehicle communication to improve roads safety.
- EVA has an ongoing collaboration with SODEAL company, which runs the Cap d'Agde marina, as part of Falco startup.
- EVA has an ongoing collaboration with SELOR company, which runs the Lorient marinas, as part of the Falco startup.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

The H2020 following project is ongoing:

- H2020 SPARTA, Jan 2019 – December 2020.

9.2.2. Collaborations in European Programs, Except FP7 & H2020

Inria-EVA has collaboration in 2018 with ETSI (the European Telecommunications Standards Institute) to organize the F-Interop 6TiSCH 2 Interop Event on 2-4 February 2018 in Paris.

9.3. International Initiatives

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

9.3.1.1. REALMS

- Title: Real-Time Real-World Monitoring Systems
- International Partner (Institution - Laboratory - Researcher):
  - University of California Berkeley (United States) - Civil and Environmental Engineering - Steven Glaser
  - University of Michigan (United States) - Civil and Environmental Engineering - Branko Kerkez
- Start year: 2015
- See also: http://glaser.berkeley.edu et http://www-personal.umich.edu/~bkerkez/
- The Internet of Things revolution prompted the development of new products and standards; The IEEE 802.15.4e (2012) standard introduced the Time Synchronized Channel Hoping (TSCH) which can provide end-to-end reliability of 99.999 % and an energy autonomy of many years. This exceptional performance prompted the IETF to create the 6TISCH working group to standardize the integration of TSCH networks in the Internet. While the first experimental data have highlighted the great robustness of these networks, there is no data of a real network, accessible in real time, on a large scale and over a long period. Such data is needed to better model network performance and produce better products and standards. The teams of Professors Glaser and Kerkez are successfully deploying such networks to study mountain hydrology, monitor water quality and manage rainwater in urban environments. A model is missing to assist in the deployment and operation of these networks, as well as to monitor an operational network.

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

Inria-EVA has a long-standing Memorandum of Understanding with the OpenMote company (http://www.openmote.com/), which runs until 2020. OpenMote emerged as a spin-off of the OpenWSN project, co-led by **Thomas Watteyne** and Prof. Xavier Vilajosana, Professor at the Open University of Catalonia and Chief Technical Officer at OpenMote.

The collaboration has been ongoing since 2012 and at the time of writing has resulted in:

- Joint academic publications, including 7 journal articles, 1 letter, 1 book chapter, 5 conference papers, 2 tutorials and invited talks.
- Joint standardization activities, in particular in the IETF 6TiSCH working group, co-chaired by **Thomas Watteyne** and for which Prof. Xavier Vilajosana is a key contributor. This activity has resulted in the joint participation in 12 IETF face-to-face meetings, joint participation in over 100 audioconferences, co-authorship of 3 Internet-Drafts and joint organization of 2 interop events.
- Joint software development, as both institutions closely collaborate in the maintenance, development, promotion and research along the OpenWSN project, including the development of the protocol stack, the integration of novel hardware technologies, the support to the community and the participation in standardization activities and interoperability events.

This MOU is NOT a commitment of funds by any party.

9.3.2.2. Informal International Partners

The Inria-EVA team collaborates extensively with Prof. Pister's group at UC Berkeley on the OpenWSN and Smart Dust projects. This activity translated into several members of the Pister team visiting Inria-EVA and vice-versa in 2018.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

1. **Martina Brachmann (RISE, Sweden)** (November 2019) working on TSCH on the RISE: Current Research and Future Directions in Networked Embedded Systems with Thomas Watteyne, Malisa Vucinic, Tengfei Chang
2. **Ana Laura Diedrichs (UTN, Argentina)** (Oct-Nov 2019) working on WirelessWine with Thomas Watteyne, Keoma Brun-Laguna
3. **Prof Leila Seidane Azouz** 1-30 October 2019 working with **Pascale Minet** and **Paul Muhlethaler** on wireless networks.
4. **Prof Ruben Milocco** visited EVA from 1-30 October 2019 working with **Pascale Minet** on evaluation of data center performance and **Paul Muhlethaler** on wireless network relaying.
5. **Prof. Diego Dujovne (UDP, Chile)** (July 2019) working on WirelessWine with Thomas Watteyne
6. **Prof. Branko Kerkez (U. Michigan)** (May 2019) working on REALMS associate team with Thomas Watteyne
7. **Mikolaj Chwalisz (TU Berlin)** (May 2019) working on Towards efficient coexistence of IEEE 802.15.4e TSCH and IEEE 802.11 Collaboration with Tengfei Chang, Thomas Watteyne

9.4.1.1. Internships

1. Amy Hane, Intern, from Sep 2019 until Dec 2019
2. Camilo Andres Lopez Lopez, Intern, from May 2019 until Aug 2019
3. Ba Hai Le, Intern, Apr-Aug 2019
4. Victor Kenichi Nascimento Kobayashi,Intern, from May 2019 until Aug 2019
5. Sharut Gupta, Intern, from May 2019 until July 2019
6. Miguel Landry Foko Sindjoung, Intern, from Mar 2019 until Jun 2019.

9.4.1.2. Research Stays Abroad

- **Thomas Watteyne** spent the month of August 2019 at UC Berkeley, working with Prof. Glaser on the SnowHow project, and with Prof. Pister on Smart Dust and OpenWSN.
- Tengfei Chang spent June 2019 in California working with Prof. Pister working on Smart Dust UC Berkeley.

GANG Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR DESCARTES

Participants: Carole Gallet Delporte, Hugues Fauconnier, Pierre Fraigniaud, Adrian Kosowski, Laurent Viennot.

Cyril Gavoille (U. Bordeaux) leads this project that grants 1 Post-Doc. H. Fauconnier is the local coordinator (This project began in October 2016).

Despite the practical interests of reusable frameworks for implementing specific distributed services, many of these frameworks still lack solid theoretical bases, and only provide partial solutions for a narrow range of services. We argue that this is mainly due to the lack of a generic framework that is able to unify the large body of fundamental knowledge on distributed computation that has been acquired over the last 40 years. The DESCARTES project aims at bridging this gap, by developing a systematic model of distributed computation that organizes the functionalities of a distributed computing system into reusable modular constructs assembled via well-defined mechanisms that maintain sound theoretical guarantees on the resulting system. DESCARTES arises from the strong belief that distributed computing is now mature enough to resolve the tension between the social needs for distributed computing systems, and the lack of a fundamentally sound and systematic way to realize these systems.

8.1.2. ANR MultiMod

Participants: Adrian Kosowski, Laurent Viennot.

David Coudert (Sophia Antipolis) leads this project. L. Viennot coordinates locally. The project began in 2018.

The MultiMod project aims at enhancing the mobility of citizens in urban areas by providing them, through a unique interface enabling to express their preferences, the most convenient transportation means to reach their destinations. Indeed, the increasing involvement of actors and authorities in the deployment of more responsible and cost-effective logistics and the progress made in the field of digital technology have made possible to create synergies in the creation of innovative services for improving the mobility in cities. However, users are faced with a number of solutions that coexist at different scales, providing complementary information for the mobility of users, but that make very complex to find the most convenient itinerary at a given time for a specific user. In this context, MultiMod aims at improving the mobility of citizens in urban areas by proposing contextualized services, linking users, to facilitate multimodal transport by combining, with flexibility, all available modes (planned/dynamic carpooling, public transport (PT), car-sharing, bicycle, etc.).

We consider the use of carpooling in metropolitan areas, and so for short journeys. Such usage enables itineraries that are not possible with PT, allows for opening up areas with low PT coverage by bringing users near PT (last miles), and for faster travel-time when existing PT itineraries are too complex or with too low frequency (e.g., one bus per hour). In this context, the application must help the driver and the passenger as much as possible. In particular, the application must propose the meeting-point, indicate the driver the detour duration, and indicate the passenger how to reach this meeting-point using PT. Here, the time taken by drivers and passengers to agree becomes a critical issue and so the application must provide all needed information to quickly take a decision (i.e., in one click).

In addition, the era of Smart City gathers many emerging concepts, driven by innovative technological players, which enables the exploitation of real-time data (e.g., delay of a bus, traffic jam) made available by the various actors (e.g., communities in the framework of Open Data projects, users via their mobile terminals, traffic supervision authorities). In the MultiMod project, we will use these rich sources of data to propose itineraries that are feasible at query-time. Our findings will enable the design of a mobility companion able not only to guide the user along her journey, including when and how to change of transportation mean, but also to propose itinerary changes when the current one exceeds a threshold delay. The main originality of this project is thus to address the problem of computing itineraries in large-scale networks combining PT, carpooling and real-time data, and to satisfy the preferences of users. We envision that the outcome of this project will significantly improve the daily life of citizens.

The targeted metropolitan area for validating our solutions is Ile-de-France. Indeed, Instant-System is currently developing the new application "Vianavigo lab" which will replace the current "Vianavigo" application for the PT network of Ile-de-France. Our findings will therefore be tested at scale and eventually be integrated and deployed in production servers and mobile applications. The smaller networks of Bordeaux and Nice will be used to perform preliminary evaluations since Instant System already operates applications in these cities (Boogi Nice, Boogi Bordeaux). An important remark is that new features and algorithms can contractually be deployed in production every 4 months, thus enabling Instant System to measure and challenge the results of the MultiMod project in continue. This is a chance for the project to maximize its impact.

8.1.3. ANR FREDDA

Participants: Carole Gallet Delporte, Hugues Fauconnier, Pierre Fraigniaud.

Arnaud Sangnier (IRIF, Univ Paris Diderot) leads this project that grants 1 PhD. (This project began in October 2017).

Distributed algorithms are nowadays omnipresent in most systems and applications. It is of utmost importance to develop algorithmic solutions that are both robust and flexible, to be used in large scale applications. Currently, distributed algorithms are developed under precise assumptions on their execution context: synchronicity, bounds on the number of failures, etc. The robustness of distributed algorithms is a challenging problem that has not been much considered until now, and there is no systematic way to guarantee or verify the behavior of an algorithm beyond the context for which it has been designed. We propose to develop automated formal method techniques to verify the robustness of distributed algorithms and to support the development of robust applications. Our methods are of two kinds: statically through classical verification, and dynamically, by synthesizing distributed monitors, that check either correctness or the validity of the context hypotheses at runtime.

8.1.4. ANR Distancia

Participants: Pierre Charbit, Michel Habib, Laurent Viennot.

Victor Chepoi (Univ. Marseille) leads this project. P. Charbit coordinates locally. The project began in early-2018.

The theme of the project is Metric Graph Theory, and we are concerned both on theoretical foundations and applications. Such applications can be found in real world networks. For example, the hub labelling problem in road networks can be directly applied to car navigation applications. Understanding key structural properties of large-scale data networks is crucial for analyzing and optimizing their performance, as well as improving their reliability and security. In prior empirical and theoretical studies researchers have mainly focused on features such as small world phenomenon, power law degree distribution, navigability, and high clustering coefficients. Although those features are interesting and important, the impact of intrinsic geometric and topological features of large-scale data networks on performance, reliability and security is of much greater importance. Recently, there has been a surge of empirical works measuring and analyzing geometric characteristics of real-world networks, namely the Gromov hyperbolicity (called also the negative curvature) of the network. It has been shown that a number of data networks, including Internet application networks, web networks, collaboration networks, social networks, and others, have small hyperbolicity.

Metric graph theory was also indispensable in solving some open questions in concurrency and learning theory in computer science and geometric group theory in mathematics. Median graphs are exactly the 1–skeletons of CAT(0) cube complexes (which have been characterized by Gromov in a local-to-global combinatorial way). They play a vital role in geometric group theory (for example, in the recent solution of the famous Virtual Haken Conjecture). Median graphs are also the domains of event structures of Winskel, one of the basic abstract models of concurrency. This correspondence is very useful in dealing with questions on event structures.

Many classical algorithmic problems concern distances: shortest path, center and diameter, Voronoi diagrams, TSP, clustering, etc. Algorithmic and combinatorial problems related to distances also occur in data analysis. Low-distortion embeddings into l1-spaces (theorem of Bourgain and its algorithmical use by Linial et al.) were the founding tools in metric methods. Recently, several approximation algorithms for NP-hard problems were designed using metric methods. Other important algorithmic graph problems related to distances concern the construction of sparse subgraphs approximating inter-node distances and the converse, augmentation problems with distance constraints. Finally, in the distributed setting, an important problem is that of designing compact data structures allowing very fast computation of inter- node distances or routing along shortest or almost shortest paths. Besides computer science and mathematics, applications of structures involving distances can be found in archeology, computational biology, statistics, data analysis, etc. The problem of characterizing isometric subgraphs of hypercubes has its origin in communication theory and linguistics. . To take into account the recombination effect in genetic data, the mathematicians Bandelt and Dress developed in 1991 the theory of canonical decompositions of finite metric spaces. Together with geneticists, Bandelt successfully used it over the years to reconstruct phylogenies, in the evolutional analysis of mtDNA data in human genetics. One important step in their method is to build a reduced median network that spans the data but still contains all most parsimonious trees. As mentioned above, the median graphs occurring there constitute a central notion in metric graph theory.

With this project, we aim to participate at the elaboration of this new domain of Metric Graph Theory, which requires experts and knowledge in combinatorics (graphs, matroids), geometry, and algorithms. This expertise is distributed over the members of the consortium and a part of the success of our project it will be to share these knowledges among all the members of the consortium. This way we will create a strong group in France on graphs and metrics.

8.1.5. ANR HOSIGRA

Participants: Pierre Charbit, Michel Habib.

This project starting in early-2018, led by Reza Naserasr, explores the connection between minors and colorings, exploiting the notion of signed graphs. With the four colour theorem playing a central role in development of Graph Theory, the notions of minor and coloring have been branded as two of the most distinguished concepts in this field. The geometric notion of planarity has given birth to the theory of minors among others, and coloring have proven to have an algebraic nature through its extension to the theory of graph homomorphisms. Great many projects have been completed on both subjects, but what remains mostly a mystery is the correlation of the two subjects. The four color theorem itself, in slightly stronger form, claims that if a complete graph on five vertices cannot be formed by minor operation from a given graph, then the graph can be homomorphically mapped into the complete graph on four vertices (thus a 4-coloring). Commonly regarded as the most challenging conjecture on graph theory, the Hadwiger conjecture claims that five and four in this theorem can be replaced with n and $n-1$ respectively for any value of n. The correlation of these two concepts has been difficult to study, mainly for the following reason: While the coloring or homomorphism problems roots back into intersections of odd-cycles, the minor operation is irrelevant of the parity of cycles. To overcome this barrier, the notion of signed graphs has been used implicitly since 1970s when coloring results on graphs with no odd-K4 is proved, following which a stronger form of the Hadwiger conjecture, known as Odd Hadwiger conjecture, was proposed by P. Seymour and B. Gerards, independently. Being a natural subclass of Matroids and a superclass of graphs, the notion of minor of signed graphs is well studied and many results from graph minor are either already extended to signed graphs or it is considered by experts of the subject. Observing the importance, and guided by some earlier works, in particular that of B.

Guenin, we then started the study of algebraic concepts (coloring and homomormphisms) for signed graphs. Several results have been obtained in the past decade, and this project aims at exploring more of this topic.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Amos Korman has an ERC Consolidator Grant entitled "Distributed Biological Algorithms (DBA)", started in May 2015. This project proposes a new application for computational reasoning. More specifically, the purpose of this interdisciplinary project is to demonstrate the usefulness of an algorithmic perspective in studies of complex biological systems. We focus on the domain of collective behavior, and demonstrate the benefits of using techniques from the field of theoretical distributed computing in order to establish algorithmic insights regarding the behavior of biological ensembles. The project includes three related tasks, for which we have already obtained promising preliminary results. Each task contains a purely theoretical algorithmic component as well as one which integrates theoretical algorithmic studies with experiments. Most experiments are strategically designed by the PI based on computational insights, and are physically conducted by experimental biologists that have been carefully chosen by the PI. In turn, experimental outcomes will be theoretically analyzed via an algorithmic perspective. By this integration, we aim at deciphering how a biological individual (such as an ant) "thinks", without having direct access to the neurological process within its brain, and how such limited individuals assemble into ensembles that appear to be far greater than the sum of their parts. The ultimate vision behind this project is to enable the formation of a new scientific field, called algorithmic biology, that bases biological studies on theoretical algorithmic insights.

8.2.2. LIA Struco

Pierre Charbit is director of the LIA STRUCO, which is an Associated International Laboratory of CNRS between IÚUK, Prague, and IRIF, Paris. The director on the Czech side is Pr. Jaroslav Nešetřil. The primary theme of the laboratory is graph theory, more specifically: sparsity of graphs (nowhere dense classes of graphs, bounded expansion classes of graphs), extremal graph theory, graph coloring, Ramsey theory, universality and morphism duality, graph and matroid algorithms and model checking.

STRUCO focuses on high-level study of fundamental combinatorial objects, with a particular emphasis on comprehending and disseminating the state-of-the-art theories and techniques developed. The obtained insights shall be applied to obtain new results on existing problems as well as to identify directions and questions for future work.

One of the main goals of STRUCO is to provide a sustainable and reliable structure to help Czech and French researchers cooperate on long-term projects, disseminate the results to students of both countries and create links between these students more systematically. The chosen themes of the project indeed cover timely and difficult questions, for which a stable and significant cooperation structure is needed. By gathering an important number of excellent researchers and students, the LEA will create the required environment for making advances, which shall be achieved not only by short-term exchanges of researchers, but also by a strong involvement of Ph. D students in the learning of state-of-the-art techniques and in the international collaborations.

STRUCO is a natural place to federate and organize these many isolated collaborations between our two countries. Thus, the project would ensure long-term cooperations and allow young researchers (especially PhD students) to maintain the fruitful exchanges between the two countries in the future years, in a structured and federated way.

8.3. International Initiatives

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

Carole Delporte-Gallet and Hugues Fauconnier are members of the Inria-MEXICO Equipe Associée LiDiCo (At the Limits of Distributed Computability, https://sites.google.com/site/lidicoequipeassociee/).

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

Ofer Feinerman (Physics department of complex systems, Weizmann Institute of Science, Rehovot, Israel), is a team member in Amos Korman's ERC project DBA. This collaboration has been formally established by signing a contract between the CNRS and the Weizmann Institute of Science, as part of the ERC project.

Rachid Guerraoui (School of Computer and Communication Sciences, EPFL, Switzerland) maintains an active research collaboration with Gang team members (Carole Delporte, Hugues Fauconnier).

Sergio Rajsbaum (UNAM, Mexico) is a regular collaborator of the team, also involved formally in a joint French-Mexican research project (see next subsection).

Boaz Patt-Shamir (Tel Aviv University, Israel) is a regular collaborator of the team, also involved formally in a joint French-Israeli research project (see next subsection).

8.4. International Research Visitors

8.4.1. Visits to International Teams

- Laurent Viennot has visited Archontia Giannopoulou at National and Kapodistrian University of Athens from July 1st to July 7th.
- Michel Habib has visited Prof. M. Chen (Xiamen University of Technology) and Prof. Lin Cheng-Kuan (Fuzhou University) in China, 9-15 december.

GANG Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR DESCARTES

Participants: Carole Gallet Delporte, Hugues Fauconnier, Pierre Fraigniaud, Adrian Kosowski, Laurent Viennot.

Cyril Gavoille (U. Bordeaux) leads this project that grants 1 Post-Doc. H. Fauconnier is the local coordinator (This project began in October 2016).

Despite the practical interests of reusable frameworks for implementing specific distributed services, many of these frameworks still lack solid theoretical bases, and only provide partial solutions for a narrow range of services. We argue that this is mainly due to the lack of a generic framework that is able to unify the large body of fundamental knowledge on distributed computation that has been acquired over the last 40 years. The DESCARTES project aims at bridging this gap, by developing a systematic model of distributed computation that organizes the functionalities of a distributed computing system into reusable modular constructs assembled via well-defined mechanisms that maintain sound theoretical guarantees on the resulting system. DESCARTES arises from the strong belief that distributed computing is now mature enough to resolve the tension between the social needs for distributed computing systems, and the lack of a fundamentally sound and systematic way to realize these systems.

8.1.2. ANR MultiMod

Participants: Adrian Kosowski, Laurent Viennot.

David Coudert (Sophia Antipolis) leads this project. L. Viennot coordinates locally. The project began in 2018.

The MultiMod project aims at enhancing the mobility of citizens in urban areas by providing them, through a unique interface enabling to express their preferences, the most convenient transportation means to reach their destinations. Indeed, the increasing involvement of actors and authorities in the deployment of more responsible and cost-effective logistics and the progress made in the field of digital technology have made possible to create synergies in the creation of innovative services for improving the mobility in cities. However, users are faced with a number of solutions that coexist at different scales, providing complementary information for the mobility of users, but that make very complex to find the most convenient itinerary at a given time for a specific user. In this context, MultiMod aims at improving the mobility of citizens in urban areas by proposing contextualized services, linking users, to facilitate multimodal transport by combining, with flexibility, all available modes (planned/dynamic carpooling, public transport (PT), car-sharing, bicycle, etc.).

We consider the use of carpooling in metropolitan areas, and so for short journeys. Such usage enables itineraries that are not possible with PT, allows for opening up areas with low PT coverage by bringing users near PT (last miles), and for faster travel-time when existing PT itineraries are too complex or with too low frequency (e.g., one bus per hour). In this context, the application must help the driver and the passenger as much as possible. In particular, the application must propose the meeting-point, indicate the driver the detour duration, and indicate the passenger how to reach this meeting-point using PT. Here, the time taken by drivers and passengers to agree becomes a critical issue and so the application must provide all needed information to quickly take a decision (i.e., in one click).

In addition, the era of Smart City gathers many emerging concepts, driven by innovative technological players, which enables the exploitation of real-time data (e.g., delay of a bus, traffic jam) made available by the various actors (e.g., communities in the framework of Open Data projects, users via their mobile terminals, traffic supervision authorities). In the MultiMod project, we will use these rich sources of data to propose itineraries that are feasible at query-time. Our findings will enable the design of a mobility companion able not only to guide the user along her journey, including when and how to change of transportation mean, but also to propose itinerary changes when the current one exceeds a threshold delay. The main originality of this project is thus to address the problem of computing itineraries in large-scale networks combining PT, carpooling and real-time data, and to satisfy the preferences of users. We envision that the outcome of this project will significantly improve the daily life of citizens.

The targeted metropolitan area for validating our solutions is Ile-de-France. Indeed, Instant-System is currently developing the new application "Vianavigo lab" which will replace the current "Vianavigo" application for the PT network of Ile-de-France. Our findings will therefore be tested at scale and eventually be integrated and deployed in production servers and mobile applications. The smaller networks of Bordeaux and Nice will be used to perform preliminary evaluations since Instant System already operates applications in these cities (Boogi Nice, Boogi Bordeaux). An important remark is that new features and algorithms can contractually be deployed in production every 4 months, thus enabling Instant System to measure and challenge the results of the MultiMod project in continue. This is a chance for the project to maximize its impact.

8.1.3. ANR FREDDA

Participants: Carole Gallet Delporte, Hugues Fauconnier, Pierre Fraigniaud.

Arnaud Sangnier (IRIF, Univ Paris Diderot) leads this project that grants 1 PhD. (This project began in October 2017).

Distributed algorithms are nowadays omnipresent in most systems and applications. It is of utmost importance to develop algorithmic solutions that are both robust and flexible, to be used in large scale applications. Currently, distributed algorithms are developed under precise assumptions on their execution context: synchronicity, bounds on the number of failures, etc. The robustness of distributed algorithms is a challenging problem that has not been much considered until now, and there is no systematic way to guarantee or verify the behavior of an algorithm beyond the context for which it has been designed. We propose to develop automated formal method techniques to verify the robustness of distributed algorithms and to support the development of robust applications. Our methods are of two kinds: statically through classical verification, and dynamically, by synthesizing distributed monitors, that check either correctness or the validity of the context hypotheses at runtime.

8.1.4. ANR Distancia

Participants: Pierre Charbit, Michel Habib, Laurent Viennot.

Victor Chepoi (Univ. Marseille) leads this project. P. Charbit coordinates locally. The project began in early-2018.

The theme of the project is Metric Graph Theory, and we are concerned both on theoretical foundations and applications. Such applications can be found in real world networks. For example, the hub labelling problem in road networks can be directly applied to car navigation applications. Understanding key structural properties of large-scale data networks is crucial for analyzing and optimizing their performance, as well as improving their reliability and security. In prior empirical and theoretical studies researchers have mainly focused on features such as small world phenomenon, power law degree distribution, navigability, and high clustering coefficients. Although those features are interesting and important, the impact of intrinsic geometric and topological features of large-scale data networks on performance, reliability and security is of much greater importance. Recently, there has been a surge of empirical works measuring and analyzing geometric characteristics of real-world networks, namely the Gromov hyperbolicity (called also the negative curvature) of the network. It has been shown that a number of data networks, including Internet application networks, web networks, collaboration networks, social networks, and others, have small hyperbolicity.

Metric graph theory was also indispensable in solving some open questions in concurrency and learning theory in computer science and geometric group theory in mathematics. Median graphs are exactly the 1–skeletons of CAT(0) cube complexes (which have been characterized by Gromov in a local-to-global combinatorial way). They play a vital role in geometric group theory (for example, in the recent solution of the famous Virtual Haken Conjecture). Median graphs are also the domains of event structures of Winskel, one of the basic abstract models of concurrency. This correspondence is very useful in dealing with questions on event structures.

Many classical algorithmic problems concern distances: shortest path, center and diameter, Voronoi diagrams, TSP, clustering, etc. Algorithmic and combinatorial problems related to distances also occur in data analysis. Low-distortion embeddings into l1-spaces (theorem of Bourgain and its algorithmical use by Linial et al.) were the founding tools in metric methods. Recently, several approximation algorithms for NP-hard problems were designed using metric methods. Other important algorithmic graph problems related to distances concern the construction of sparse subgraphs approximating inter-node distances and the converse, augmentation problems with distance constraints. Finally, in the distributed setting, an important problem is that of designing compact data structures allowing very fast computation of inter- node distances or routing along shortest or almost shortest paths. Besides computer science and mathematics, applications of structures involving distances can be found in archeology, computational biology, statistics, data analysis, etc. The problem of characterizing isometric subgraphs of hypercubes has its origin in communication theory and linguistics. . To take into account the recombination effect in genetic data, the mathematicians Bandelt and Dress developed in 1991 the theory of canonical decompositions of finite metric spaces. Together with geneticists, Bandelt successfully used it over the years to reconstruct phylogenies, in the evolutional analysis of mtDNA data in human genetics. One important step in their method is to build a reduced median network that spans the data but still contains all most parsimonious trees. As mentioned above, the median graphs occurring there constitute a central notion in metric graph theory.

With this project, we aim to participate at the elaboration of this new domain of Metric Graph Theory, which requires experts and knowledge in combinatorics (graphs, matroids), geometry, and algorithms. This expertise is distributed over the members of the consortium and a part of the success of our project it will be to share these knowledges among all the members of the consortium. This way we will create a strong group in France on graphs and metrics.

8.1.5. ANR HOSIGRA

Participants: Pierre Charbit, Michel Habib.

This project starting in early-2018, led by Reza Naserasr, explores the connection between minors and colorings, exploiting the notion of signed graphs. With the four colour theorem playing a central role in development of Graph Theory, the notions of minor and coloring have been branded as two of the most distinguished concepts in this field. The geometric notion of planarity has given birth to the theory of minors among others, and coloring have proven to have an algebraic nature through its extension to the theory of graph homomorphisms. Great many projects have been completed on both subjects, but what remains mostly a mystery is the correlation of the two subjects. The four color theorem itself, in slightly stronger form, claims that if a complete graph on five vertices cannot be formed by minor operation from a given graph, then the graph can be homomorphically mapped into the complete graph on four vertices (thus a 4-coloring). Commonly regarded as the most challenging conjecture on graph theory, the Hadwiger conjecture claims that five and four in this theorem can be replaced with n and $n-1$ respectively for any value of n. The correlation of these two concepts has been difficult to study, mainly for the following reason: While the coloring or homomorphism problems roots back into intersections of odd-cycles, the minor operation is irrelevant of the parity of cycles. To overcome this barrier, the notion of signed graphs has been used implicitly since 1970s when coloring results on graphs with no odd-K4 is proved, following which a stronger form of the Hadwiger conjecture, known as Odd Hadwiger conjecture, was proposed by P. Seymour and B. Gerards, independently. Being a natural subclass of Matroids and a superclass of graphs, the notion of minor of signed graphs is well studied and many results from graph minor are either already extended to signed graphs or it is considered by experts of the subject. Observing the importance, and guided by some earlier works, in particular that of B.

Guenin, we then started the study of algebraic concepts (coloring and homomormphisms) for signed graphs. Several results have been obtained in the past decade, and this project aims at exploring more of this topic.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Amos Korman has an ERC Consolidator Grant entitled "Distributed Biological Algorithms (DBA)", started in May 2015. This project proposes a new application for computational reasoning. More specifically, the purpose of this interdisciplinary project is to demonstrate the usefulness of an algorithmic perspective in studies of complex biological systems. We focus on the domain of collective behavior, and demonstrate the benefits of using techniques from the field of theoretical distributed computing in order to establish algorithmic insights regarding the behavior of biological ensembles. The project includes three related tasks, for which we have already obtained promising preliminary results. Each task contains a purely theoretical algorithmic component as well as one which integrates theoretical algorithmic studies with experiments. Most experiments are strategically designed by the PI based on computational insights, and are physically conducted by experimental biologists that have been carefully chosen by the PI. In turn, experimental outcomes will be theoretically analyzed via an algorithmic perspective. By this integration, we aim at deciphering how a biological individual (such as an ant) "thinks", without having direct access to the neurological process within its brain, and how such limited individuals assemble into ensembles that appear to be far greater than the sum of their parts. The ultimate vision behind this project is to enable the formation of a new scientific field, called algorithmic biology, that bases biological studies on theoretical algorithmic insights.

8.2.2. LIA Struco

Pierre Charbit is director of the LIA STRUCO, which is an Associated International Laboratory of CNRS between IÚUK, Prague, and IRIF, Paris. The director on the Czech side is Pr. Jaroslav Nešetřil. The primary theme of the laboratory is graph theory, more specifically: sparsity of graphs (nowhere dense classes of graphs, bounded expansion classes of graphs), extremal graph theory, graph coloring, Ramsey theory, universality and morphism duality, graph and matroid algorithms and model checking.

STRUCO focuses on high-level study of fundamental combinatorial objects, with a particular emphasis on comprehending and disseminating the state-of-the-art theories and techniques developed. The obtained insights shall be applied to obtain new results on existing problems as well as to identify directions and questions for future work.

One of the main goals of STRUCO is to provide a sustainable and reliable structure to help Czech and French researchers cooperate on long-term projects, disseminate the results to students of both countries and create links between these students more systematically. The chosen themes of the project indeed cover timely and difficult questions, for which a stable and significant cooperation structure is needed. By gathering an important number of excellent researchers and students, the LEA will create the required environment for making advances, which shall be achieved not only by short-term exchanges of researchers, but also by a strong involvement of Ph. D students in the learning of state-of-the-art techniques and in the international collaborations.

STRUCO is a natural place to federate and organize these many isolated collaborations between our two countries. Thus, the project would ensure long-term cooperations and allow young researchers (especially PhD students) to maintain the fruitful exchanges between the two countries in the future years, in a structured and federated way.

8.3. International Initiatives

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

Carole Delporte-Gallet and Hugues Fauconnier are members of the Inria-MEXICO Equipe Associée LiDiCo (At the Limits of Distributed Computability, https://sites.google.com/site/lidicoequipeassociee/).

8.3.2. Inria International Partners

8.3.2.1. Informal International Partners

Ofer Feinerman (Physics department of complex systems, Weizmann Institute of Science, Rehovot, Israel), is a team member in Amos Korman's ERC project DBA. This collaboration has been formally established by signing a contract between the CNRS and the Weizmann Institute of Science, as part of the ERC project.

Rachid Guerraoui (School of Computer and Communication Sciences, EPFL, Switzerland) maintains an active research collaboration with Gang team members (Carole Delporte, Hugues Fauconnier).

Sergio Rajsbaum (UNAM, Mexico) is a regular collaborator of the team, also involved formally in a joint French-Mexican research project (see next subsection).

Boaz Patt-Shamir (Tel Aviv University, Israel) is a regular collaborator of the team, also involved formally in a joint French-Israeli research project (see next subsection).

8.4. International Research Visitors

8.4.1. Visits to International Teams

- Laurent Viennot has visited Archontia Giannopoulou at National and Kapodistrian University of Athens from July 1st to July 7th.
- Michel Habib has visited Prof. M. Chen (Xiamen University of Technology) and Prof. Lin Cheng-Kuan (Fuzhou University) in China, 9-15 december.

KOPERNIC Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FUI

8.1.1.1. CEOS

This project was started on May 2017. Partners of the project are: ADCIS, ALERION, Aeroport de Caen, 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.

8.2. European Initiatives

8.2.1. Collaborations with Major European Organizations

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

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

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- Prof. Christopher Gill, Washington University in St. Louis (May 2019).
- Robert Davis, University of York (July 2019).

8.3.1.1. Internships

- Kartikeya Singh (India).

MAMBA Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

Mamba (Marie Doumic and Philippe Robert) participates to the GDR "MeDyna" (mechanisms and dynamics of assemblies of peptides and proteins), coordinated by Stéphane Bressanelli from IBPC.

8.1.1. ANR

8.1.1.1. ANR Blanc 2014-2018 "Kibord"

This project gathers several members of the MAMBA team together with the ENS Cachan and Université Paris-Dauphine on the mathematical study of PDE models with application to biology.

8.1.1.2. ANR iLITE 2016 - 2020

Jean-Charles Duclos-Vallée, Paul Brousse Hospital, Villejuif. Partners are several departments in Paul Brousse Hospital, ENS Cachan, University of Compiègne and several companies all over France, and COMMEDIA team, Inria Paris. The pursued objective is the bioengineering design of an artificial liver intended for liver replacement.

8.1.1.3. ANR InTelo 2017-2020

Telomere dynamics, headed by Teresa Teixeira (IBPC, Paris).

8.1.1.4. INCa/DGOS; PRT-K 2018-2021

Khê HOANG-XUAN, Hôpital Universitaire La Pitié Salpêtrière, Paris. Mathematical modeling at micro and macroscopic level of primary central nervous system lymphomas (PCNSL).

8.1.2. ITMO Cancer 2016 - 2020, HTE call (heterogeneity of tumours in their ecosystems)

8.1.2.1. ITMO Cancer EcoAML

Early leukaemogenesis in Acute Myelogenous Leukaemia (AML), 8 teams headed by François Delhommeau (CDR St Antoine, Paris).

8.1.2.2. ITMO Cancer MoGlImaging

Treatment-induced treatment resistance and heterogeneity in glioblastoma, 8 teams headed by Elizabeth Moyal (INSERM, Toulouse).

8.2. International Initiatives

- **STIC AmSud 20-STIC-05**
  - Title: New Methods for Biological Control of the Arboviruses
  - International Partner (Institution - Laboratory - Researcher):

    CIRAD (Montpellier), UMR MISTEA (Montpellier), Université Paris 13, Université de Bordeaux, Université de Strasbourg, Université Paris-Dauphine - PSL; Universidad de Buenos Aires and Universidad Nacional de Salta (Argentina); Universidad de Chile (Chile); Universidad del Quindio, Universidad Autónoma de Occidente and Universidad del Valle (Colombia); National University of Asuncion (Paraguay).
  - Duration: 2020 - 2021
  - Start year: 2020

  - The main focus of this project is modeling and analysis, using mathematical methods, of new strategies aimed at controling the spread of the dengue fever and other vector-borne diseases similar to Dengue and transmitted by Aedes mosquitoes, like Chikungunya and Zika virus.
  - The key topics are the following.
    * Spatial aspects of biological control techniques
    * Estimation issues for vector-borne epidemics
    * Optimal and non-optimal control approaches for biological control techniques
    * Modelling the effects of conventional control methods on the success of biological control
    * Modelling the competition effects in larval phase during biological control
    * Modelling and efficacy measures for self-propagating genetic interventions
    * Genome-scale models for Wolbachia

- **ERC Advanced grant No 740623 ADORA**

  ADORA is the acronym for *Asymptotic approach to spatial and dynamical organizations*.

  Adora ERC project aims at understanding of spatial, social and dynamical organization of large numbers of agents, presently a fundamental issue in science. ADORA focuses on problems motivated by biology because, more than anywhere else, access to precise and numerous data has opened the route to novel and complex mathematical models. The address ed problems are written in terms of **nonlinear partial differential equations**. The flux-limited Keller-Segel system, the integrate-and-fire Fokker-Planck equation, kinetic equations with internal state, nonlocal parabolic equations and constrained Hamilton-Jacobi equations are among examples of the equations under investigation.

  The role of mathematics is not only to understand the analytical structure of these new problems, but it is also to **explain the qualitative behavior of solutions and to quantify their properties**. The challenge arises here because these goals should be achieved through a hierarchy of scales. Indeed, the problems under consideration share the common feature that the large scale behavior cannot be understood precisely without access to a hierarchy of finer scales, down to the individual behavior and sometimes its molecular determinants.

  Major difficulties arise because the numerous scales present in these equations have to be discovered and singularities appear in the asymptotic process which yields deep compactness obstructions. Our vision is that **the complexity inherent to models of biology can be enlightened** by mathematical analysis and a classification of the possible asymptotic regimes.

  However an enormous effort is needed to uncover the equations intimate mathematical structures, and bring them at the level of conceptual understanding they deserve being given the applications motivating these questions which range from medical science or neuroscience to cell biology.

8.2.1. MaMoCeMa

Title: Mathematical modeling of cell motility and of autophagy

International Partner (Institution - Laboratory - Researcher):

University of Vienna (Austria) - Wolfgang Pauli Institute - Christian Schmeiser

Start year: 2018

Numerous fruitful collaborations have been developed these last years between the WPI and the Inria team MAMBA. Diane Peurichard – newly recruited permanent member of the team MAMBA- worked two years (2016-2017) with Christian Schmeiser -member of the present project- through a post-doctoral contract at the university of Vienna. In collaboration with the biologists of IST, they developed mathematical tools to understand how cells move through adhesion-based and adhesion-free motion with applications in cancer development, prevalent theme of the team MAMBA.

Collaborations WPI-MAMBA have been maintained and ensured by the sabbatical of Marie Doumic (2016-2018) -, working at the university of Vienna with Christian Schmeiser and the PhD student Julia Delacour. They have initiated a collaboration on the mathematical modeling of autophagy, which requires both C. Schmeiser's expertise in biomechanics and M. Doumic's knowledge on aggregation processes. This team will also benefit of the strong links that C. Schmeiser has developed with the two biologists teams of S. Martens (on autophagy) and M. Sixt (on cell movement).

8.2.2. Participation in Other International Programs

- **BMBF (Germany) / LiSym; 2016-2020** LiSym addresses liver diseases and regeneration, namely, steatosis, fibrosis and cirrhosis, and acute on chronic liver failure. (Dirk Drasdo)
- **BMBF (Germany) / MSDILI; 2016-2019** MS-DILI addresses multiscale modeling of drug-induced liver disease focusing on the role of APAP. Dirk Drasdo participates in this project. (Dirk Drasdo)

8.3. International Research Visitors

Visitors in Paris (LJLL) invited by J. Clairambault: Zineb Kaïd, PhD student, University Abou Bekr Belkaïd, Tlemcen, Nov. 25 - Dec. 13; Jean-François Mascari, researcher, IAC-CNR, Rome, Dec. 9-13.

Visitors in Paris (Inria) invited by D. Drasdo: Jieling Zhao, Postdoc from IfADo, Jules Dichamp, Postdoc from ifADo, Paul van Liedekerke, Research engineer from IfADo.

Visitors in Paris (LJLL) invited by D. Peurichard and M. Doumic: P. Degond (Imperial College London) Nov 20 - 22, C. Schmeiser (University of Vienna), Dec. 1 - 7, Claudia Wytrzen (University of Vienna) feb 4-8 2019, M. Tournus and M. Escobedo (February 18-22), .

Visitors in Paris (LJLL) invited by P. A. Bliman: Prof. Héctor Jairo Martínez Romero (Universidade del Valle, Cali, Colombia) for two weeks, together with Oscar Eduardo Escobar Lasso, PhD student who was present one month.

Visitors in Paris (LJLL) invited by B. Perthame: Shugo Yasuda (University of Hyogo, Kobe, Japan), Min Tang (SJTU, China), Maria Caceres (Granada, Spain), Zhenan Zhou (Peking University), Weizhu Bao (Singapore university).

MATHERIALS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

The project-team is involved in several ANR projects:

- S. Boyaval is the PI of the ANR JCJC project SEDIFLO (2016-2021) to investigate new numerical models of solid transport in rivers.
- V. Ehrlacher is the PI of the ANR project COMODO (2020-2024) which focuses on the development of efficient numerical methods to simulate cross-diffusion systems on moving domains, with application to the simulation of the fabrication process of thin film solar cells. It includes research teams from Inria Lille, Inria Sophia-Antipolis and Germany.
- V. Ehrlacher is a member of the ANR project ADAPT (2018-2022), PI: D. Lombardi, Inria REO team-project. This project is concerned with the parallelization of tensor methods for high-dimensional problems.
- F. Legoll is a member of the ANR project CINE-PARA (2015-2020), PI: Y. Maday, Sorbonne Université. This project is concerned with parallel-in-time algorithms.
- T. Lelièvre is responsible of the node "Ecole des Ponts" of the ANR QuAMProcs (2019-2023), to which G. Stoltz also participates, PI: L. Michel, Université de Bordeaux.
- G. Stoltz is the PI of the ANR project COSMOS (2014-2019) which focuses on the development of efficient numerical techniques to simulate high-dimensional systems in molecular dynamics and computational statistics. It includes research teams from Institut Mines-Telecom, Inria Rennes and IBPC Paris.

Members of the project-team are participating in the following GdR:

- AMORE (Advanced Model Order REduction),
- CORREL (correlated methods in electronic structure computations),
- DYNQUA (time evolution of quantum systems, with applications to transport problems, nonequilibrium systems, etc.),
- EGRIN (gravity flows),
- MANU (MAthematics for NUclear applications),
- MASCOT-NUM (stochastic methods for the analysis of numerical codes),
- MEPHY (multiphase flows),
- NBODY (electronic structure),
- REST (theoretical spectroscopy),
- CHOCOLAS (experimental and numerical study of shock waves).

The project-team is involved in two Labex: the Labex Bezout (2011-) and the Labex MMCD (2012-).

We have invited the following national researchers to visit our team:

- A. Lozinski (University of Besançon): repeated visits during the year 2019.

8.2. European Initiatives

The ERC consolidator Grant MSMATH (ERC Grant Agreement number 614492, PI T. Lelièvre) ended in June 2019.

The ERC Synergy Grant EMC2 (ERC Grant Agreement number 810367 , PI E. Cancès, L. Grigori, Y. Maday, J-P. Piquemal) has started in September 2019.

8.3. International Initiatives

T. Lelièvre, G. Stoltz and F. Legoll participate in the Laboratoire International Associé (LIA) CNRS / University of Illinois at Urbana-Champaign on complex biological systems and their simulation by high performance computers. This LIA involves French research teams from Université de Nancy, Institut de Biologie Structurale (Grenoble) and Institut de Biologie Physico-Chimique (Paris). The LIA has been renewed for 4 years, starting January 1st, 2018.

MATHRISK Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

- ANR Cosmos 2015-2018, Participant: B. Jourdain ; Partners : Ecole des Ponts, Telecom, INIRIA Rennes and IBPC
- Labex Bezout
  http://bezout.univ-paris-est.fr

9.1.1. Competitivity Clusters

Pôle Finance Innovation

9.2. International Initiatives

9.2.1. Inria International Partners

9.2.1.1. Informal International Partners

- Center of Excellence program in Mathematics and Life Sciences at the Department of Mathematics, University of Oslo, Norway, (B. Øksendal).
- Cornell University, ORIE department (Andreea Minca)
- Roma Tor Vergata University (Lucia Caramellino)
- Ritsumeikan University (A. Kohatsu-Higa).

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Oleg Kudryavtsev (Rostov University, Russia)
- B. Stemper (Weierstrass Institute, Berlin)
- A. Kohatsu Higa (Ritsumeikan University)
- Justin Kirkby (Georgia Institute of Technology, Atlanta)
- Xiao Wei (Beijing University)
- Anton Arnold (TU Vienna)

9.3.1.1. Internships

- Baba Abdel Hamid, Inria
- Asma Sassi, Inria

9.3.2. Visits to International Teams

9.3.2.1. Research Stays Abroad

In the period 15.05 - 15. 06. 2019 Vlad Bally was an invited professor at the University Tor Vergata, Roma. Here he gave a course of 20h entitled "Integration by Parts and Convergence in Total Variation".

MIMOVE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

"BottleNet: Understanding and Diagnosing End-to-end Communication Bottlenecks of the Internet", project funded by the French research agency (ANR), from Feb 2016 to Sep 2020.

9.1.1. Inria Support

9.1.1.1. Inria IPL BetterNet

Participants: Renata Teixeira, Vassilis Christophides, Giulio Grassi.

- **Name:** BetterNet – *An observatory to measure and improve Internet service access from user experience*
- **Period:** [2016 – 2019]
- **Inria teams:** Diana, Dionysos, Inria Chile, Madynes, MiMove, Spirals
- **URL:** https://project.inria.fr/betternet/

BetterNet aims at building and delivering a scientific and technical collaborative observatory to measure and improve the Internet service access as perceived by users. In this Inria Project Lab, we will propose new original user-centered measurement methods, which will associate social sciences to better understand Internet usage and the quality of services and networks. Our observatory can be defined as a vantage point, where:

1. tools, models and algorithms/heuristics will be provided to collect data,
2. acquired data will be analyzed, and shared appropriately with scientists, stakeholders and civil society,
3. and new value-added services will be proposed to end-users.

9.1.1.2. Inria ADT SocialBus

Participants: Valérie Issarny , Rafael Angarita, Nikolaos Georgantas, Ehsan Ahvar , Lior Diler .

- **Name:** SocialBus – *Contributing to the development of SocialBus - A Universal Social Network Bus*
- **Period:** [July 2018 – June 2019 ; November 2019 – October 2020]
- **Partners:** Inria MiMove.

Computer-mediated communication can be defined as any form of human communication achieved through computer technology. From its beginnings, it has been shaping the way humans interact with each other, and it has influenced many areas of society. There exist a plethora of social interaction services enabling computer-mediated social communication (e.g., Skype, Facebook Messenger, Telegram, WhatsApp, Twitter, Slack, etc.). Based on personal preferences, users may prefer a social interaction services rather than another. As a result, users sharing same interests may not be able to interact since they are using incompatible technologies.

To tackle the above interoperability barrier, we propose SocialBus, a middleware solution targeted to enable the interaction via heterogeneous social interaction services. The ADT specifically supports the related implementation through the funding an engineer, toward technology transfer in the mid-term.

The SocialBus software is available under the AGPL open source license at https://gitlab.inria.fr/usnb/universal-social-network-bus.

9.2. International Initiatives

9.2.1. Inria International Labs

Inria@EastCoast

Associate Team involved in the International Lab:

9.2.1.1. HOMENET

Title: Home network diagnosis and security

International Partner (Institution - Laboratory - Researcher):

Princeton (United States) - Computer Science - Nick Feamster

Start year: 2017

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

Modern households connect a multitude of networked devices (ranging from laptops and smartphones to a number of Internet of Things devices) via a home network. Most home networks, however, do not have a technically skilled network administrator for managing the network, for example to identify faulty equipment or take steps to secure end hosts such as applying security patches. Home networks represent a particularly challenging environment due to the diversity of devices, applications, and services users may connect. The goal of HOMENET is to assist users in diagnosing and securing their home networks. Our approach is based on developing new algorithms and mechanisms that will run on the home router (or in-collaboration with the router). The router connects the home network to the rest of the Internet; it is hence the ideal place to secure home devices and to distinguish problems that happen in the home from those happening elsewhere. We will address a number of research challenges for example in device discovery and fingerprinting, anomaly detection in the Internet of Things, home network diagnosis (including wireless diagnosis). HOMENET will bring together two leading research teams in the network measurement arena with successful prior collaboration. Moreover, Princeton brings an existing home router platform and expertise in security, wireless, and software-defined networks; and Muse brings an existing Web-based measurement platform, and expertise in traffic-based profiling and anomaly detection.

Inria@SiliconValley

Associate Team involved in the International Lab:

9.2.1.2. MINES

Title: Adaptive Communication Middleware for Resilient Sensing & Actuation IN Emergency Response Scenarios

International Partner (Institution - Laboratory - Researcher):

University of California, Irvine (United States) - Information and Computer Science - Nalini Venkatasubramanian

Start year: 2018

See also: http://mimove-apps.paris.inria.fr/mines/index.html

Emerging smart-city and smart-community efforts will require a massive deployment of connected entities (Things) to create focused smartspaces. Related applications will enhance citizen quality of life and public safety (e.g., providing safe evacuation routes in fires). However, supporting IoT deployments are heterogeneous and can be volatile and failure-prone as they are often built upon low-powered, mobile and inexpensive devices - the presence of faulty components and intermittent network connectivity, especially in emergency scenarios, tend to deliver inaccurate/delayed information. The MINES associate team addresses the resulting challenge of enabling interoperability and resilience in large-scale IoT systems through the design and development of a dedicated middleware. More specifically, focusing on emergency situations, the MINES middleware will: (i) enable the dynamic composition of IoT systems from any and all available heterogeneous devices; (ii) support the timely and reliable exchange of critical data within and across IoT in the enabled large-scale and dynamic system over heterogeneous networks. Finally, the team will evaluate the proposed solution in the context of emergency response scenario use cases.

9.2.2. Inria International Partners

9.2.2.1. Informal International Partners

- Northeastern University (Prof. David Choffnes): We are working on methods based on active probing to diagnose poor video quality.
- Universidade Federal do Rio de Janeiro, Brazil (Prof. Edmundo Souza e Silva): We are working on characterizing Internet bottlenecks.
- Universidade Federal de Goias, Brazil (Prof. Fabio Costa): We are working on service selection and cloud resource allocation for QoS-aware enactment of service choreographies.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Mark Crovella from Boston University was visiting professor at Inria.

9.3.2. Visits to International Teams

9.3.2.1. Sabbatical programme

Renata Teixeira is visiting scholar at the Computer Science Department at Stanford University.

9.3.2.2. Research Stays Abroad

Georgios Bouloukakis was Inria postdoctoral fellow at University of California, Irvine, in the context of the Inria@SiliconValley program.

MOKAPLAN Project-Team

6. Partnerships and Cooperations

6.1. National Initiatives

6.1.1. ANR

V. Duval is the PI of the CIPRESSI (ANR JCJC) project. Its aim is to develop novel numerical schemes which respect the continuous nature of the variational problems in image or signal processing.
J-D. Benamou and G. Carlier are members of the ANR MFG (ANR-16-CE40-0015-01). Scientific topics of the project: Mean field analysis Analysis of the MFG systems and of the Master equation Numerical analysis Models and applications
J-D. Benamou G. Carlier F-X. Vialard and T. O. Gallouët are members of ANR MAGA (ANR-13-JS01-0007-01). The Monge-Ampère equation is a fully nonlinear elliptic equation, which plays a central role in geometry and in the theory of optimal transport. However, the singular and non-linear nature of the equation is a serious obstruction to its efficient numerical resolution. The first aim of the MAGA project is to study and to implement discretizations of optimal transport and Monge-Ampère equations which rely on tools from computational geometry (Laguerre diagrams). In a second step, these solvers will be applied to concrete problems from various fields involving optimal transport or Monge-Ampère equations such as computational physics: early universe reconstruction problem, congestion/incompressibility constraints economics: principal agent problems, geometry: variational problems over convex bodies, reflector and refractor design for non-imaging optics
T. O. Gallouët is member of the ANR GEOPOR (JCJC of C. Cancès) Scientific topic: geometrical approach, based on Wasserstein gradient flow, for multiphase flows in porous media. Theory and Numerics.
T. O. Gallouët is member of the ANR MESA (JCJC of M. Fathi) Scientific topic: Stein methods.

6.2. European Initiatives

6.2.1. FP7 & H2020 Projects

J-D. Benamou and Giorgi Rukhaia are members of ROMSOC ITN-EID.

6.3. International Initiatives

6.3.1. Inria International Partners

6.3.1.1. Informal International Partners

The team has strong ties with Technische Universität München, dept. of Math. (Profs. Daniel Matthes, Gero Friesecke, Bernhardt Schmitzer)

6.4. International Research Visitors

6.4.1. Visits of International Scientists

15-28/02 Visit of Prof. Yanir Rubinstein (University of Maryland).

6.4.2. Visits to International Teams

6.4.2.1. Research Stays Abroad

P. Pegon has been invited by Maria Colombo (Chair of Mathematical Analysis, Calculus of Variations and PDEs) at EPFL, Lausanne for 4 months (Feb-June 2019) to work on optimal and branched transport problems.

OURAGAN Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

- FMJH Program, PGMO grant

  ALMA (Algebraic methods in games and optimization).

  Duration: 2018 – 2020. (2 years project)

  Coordinator: Elias Tsigaridas, with Stéphane Gaubert and Xavier Allamigeon (CMAP, École Polytechnique)

9.1.1. ANR

- ANR JCJC GALOP (Games through the lens of ALgebra and OPptimization)

  Coordinator: Elias Tsigaridas

  Duration: 2018 – 2022

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

9.2. European Initiatives

9.2.1. 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.

9.3. International Initiatives

- Partenariat Hubert Curien franco-turc (PHC Bosphore) with Gebze Technical University, Turkey.

  Title: "Gröbner bases, ResultAnts and Polyhedral gEometry" (GRAPE)

  Duration: 2019 – 2020 (2 years project)

  Coordinator: Elias Tsigaridas

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

9.3.1.1. MACAO

Title: Mathematics and Algorithms for Cryptographic Advanced Objects

International Partner (Institution - Laboratory - Researcher):

University of Wollongong (Australia) - Thomas Plantard

Start year: 2019

See also: https://ssl.informatics.uow.edu.au/MACAO/

Since quantum computers have the ability to break the two main problems on which current public cryptography relies, i.e., the factoring and discrete logarithm problem, every step towards the practical realization of these computers raises fears about potential attacks on cryptographic systems. By scrutinizing the techniques proposed to build post-quantum cryptography, we can identify a few candidate hard problems which underly the proposals. One objective of this international project is to precisely assess the security of these cryptographic algorithms. First, by analyzing in a systematic manner the existing resolution algorithms and by assessing their complexity as a function of security parameters. Then, we will consider new algorithmic techniques to solve these candidate hard Post-Quantum problems, both on classical computers and quantum machines aiming at the discovery of new and better algorithms to solve them.

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

- University of Wollongong (Australia)

9.3.2.2. 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 (Alex. Kobel)
- Holon Institute of Technology, Israel (Jeremy Kaminsky)
- Department of Informatics, National Kapodistrian University of Athens, Greece (Ioannis Emiris)

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

The ANR JCJC project "FidelR" was awarded to Timothy Bourke this year and will begin in 2020.

8.1.1.1. ANR/CHIST-ERA DIVIDEND project, 2013-2019.

This project continues.

8.1.2. FUI: Fonds unique interministériel

8.1.2.1. 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. Programme d'Investissements d'Avenir (PIA)

8.1.3.1. ES3CAP collaborative project (Bpifrance)

Develop a software and hardware platform for tomorrow's intelligent systems. PARKAS collaborates with the industrial participants ANSYS/Esterel Technologies, Kalray, and Safran Electronics & Defense. Inria contacts are Marc Pouzet (PARKAS, Paris) and Fabrice Rastello (CORSE, Grenoble).

8.1.4. Others

8.1.4.1. Inria Project Lab (IPL) Modeliscale

This project 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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

- MNEMOSENE is a project with funding from the European Union's Horizon 2020 Research and Innovation Programme. Its objectives include the improvement of the energy-delay product, the computational efficiency and performance density by several orders of magnitude compared to state-of-the-art architectures. A cornerstone of the proposed solution is the memristor-based Compute-in-Memory (CIM) architecture, which eliminates long-distance, high-latency data transfers between memory and computing units required in conventional Von Neumann-based architectures by carrying out computations for performance-critical operations directly in memory.
- TETRAMAX, *Technology Transfer via Multinational Application Experiments*, is funded by the H2020 "Smart Anything Everywhere (SAE)" initiative. The overall ambition is to build and leverage 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.

8.3. International Initiatives

8.3.1. 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).

PI.R2 Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

Pierre-Louis Curien, Emilio J. Gallego Arias, 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 until Sept. 2019) 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.

Yves Guiraud will coordinate the four-year Action Exploratoire Inria Réal (Réécriture Algébrique), starting in January 2020. Its aim is to continue the unification of rewriting-like methods in abtract and higher algebra, with a view toward applications in homological and higher algebra, and group and representation theory. This investigation is pursued in immersion at IMJ-PRG, the fundamental maths common laboratory of Sorbonne Université and Université Paris Diderot.

Emilio J. Gallego Arias is a member of the GDR Génie de la Programation et du Logiciel, in the LTP (Langages, Types et Preuves) group.

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 collaborates with Nomadic Labs on the topic of certified smart contract compilation.

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 and ended in September 2019. 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, ending in 2020. The PhD grant of Antoine Allioux is funded by the CoqHoTT ERC.

8.2. European Initiatives

8.2.1. 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: March 2016 - March 2020
- Coordinator: Herman Geuvers
- Other partners: 29 countries
- Abstract: This COST promotes (1) the synergy between theoretical computer scientists, logicians and mathematicians to develop new foundations for 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.

8.3. International Initiatives

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

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. This project was renewed in 2019 for a duration of two years.

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.

8.3.2. Inria International Partners

8.3.2.1. Participation in International Programs

Pierre-Louis Curien and Alexis Saurin are members of CNRS GDRI-LL a french-italian network on linear logic community in France and Italy.

8.3.2.2. International Initiatives

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" (December 2017 – December 2020). 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).

8.4. International Research Visitors

8.4.1. Research Stays Abroad

Matthieu Sozeau visited the Programming Languages group of Benjamin Pierce at the University of Pennsylvania in June and July 2019, along with visits at MIT and Princeton to other members of the NSF DeepSpec project.

Pierre-Louis Curien visited East China Normal University (ECNU), Shanghai, for a month from early October to early December 2019 as invited professor.

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

  COMPUTER ALGEBRA METHODS FOR SEMI-ALGEBRAIC PROGRAMMING

  `Participants:` J. Berthomieu [contact], M. Safey El Din.

  Semi-Algebraic Programming is the art of optimizing some quantity subject to semi-algebraic constraints. The very basic and natural instance of semi-algebraic programming is the problem of optimizating a polynomial function subject to polynomial inequalities and is known as the polynomial optimization problem (POP). More general instances of semi-algebraic programming are as follows: given a system of polynomial equations/inequalities depending on parameters, what are the parameters' values which maximize the dimension of the semi-algebraic set defined by the instantiated system? And when the number of solutions is finite, what is this maximum number of solutions? Hence Semi-Algebraic Programming encompasses a wide range of computational issues related to semi-algebraic sets. It finds applications in many engineering sciences. Let us mention the few ones that we target in CAMiSAdo: Path-planning optimization in robotics, Mobility properties of manipulators in mechanism design, Stability analysis for sensor-based controllers.

8.2. National Initiatives

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

  `Duration:` 2018–2022

  `Participants:` J.-C. Faugère, M. Safey El Din [contact].

  The demand for flexible, adaptable robots capable of interacting with their environment (e.g. navigation, handling, cooperation) is growing. This is why the sensor-based controllers, which make it possible to include external sensory feedback in robot control, have been widely developed in recent years, both for industrial, medical, air, space and marine robotics and in the context of autonomous vehicles (ground mobile robotics).

  The first research on sensor-based control techniques took place at the end of the 1980s, with the use of proximal and force and vision sensors, and much work has been done to improve the performance of this type of controllers, in particular by modelling various sensor primitives.

  Despite the fact that, empirically, sensor-based controllers have shown that they have interesting performances, these performances are by no means guaranteed, which is a major obstacle to the widespread use of their large-scale use. This is related to the fact that, despite three decades of research on the subject, two broad classes of problems have been little explored:

  – The study of the singularities of sensor-based controllers
  – The study of their stability.

  The objectives of the project SESAME are take advantage on recent mathematical advances in order to:

  – study singularities and stability of certain classes of sensor-based controllers
  – synthesize globally asymptotically stable sensor-based controllers, whose performance (i.e. convergence properties towards the desired configuration, abseance of local singularities and minima) are guaranteed in all object/sensor related configurations.

Many of the computational tools SESAME relies on involve computer algebra and polynomial system solving.

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

  `Duration:` 2018–2022

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

  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.

- **ANR ECARP (Efficient Certified Algorithms for Robot Motion Planning)**

  `Duration:` 2020–2024

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

  ECARP is an international project, jointly funded by ANR and FWF (the funding agency of Austria). It targets the design and implementation of high-performance computer algebra algorithms for semi-algebraic sets in order to answer connectivity queries over those sets. This is applied to motion planning issues in robotics, e.g. for analyzing kinematic singularities ; parallel and serial manipulators will be investigated. The consortium gathers experts in geometry and robotics from J. Kepler Univ. (Austria) and LS2N (Nantes).

- **ANR DRN (DeRerumNatura)**

  `Duration:` 2020–2024

  `Participants:` J. Berthomieu [contact], M. Safey El Din.

  Classifying objects, determining their nature is more often than not the endgame of a theory. Yet, even the most established theory can be impractible on a concrete instance, either because of a lack of efficiency or because of a computational wall. In both cases, an algorithm is lacking: we need to systematize efficiently and automatically. This is what DRN proposes to do to solve classification problems related to numbers, analytic functions and combinactorics generating series. The consortium gathers experts in computer algebra (Inria Saclay, Limoges, Lyon, POLSYS), Combinactorics (Inria Saclay, Lyon) and Galois Theory (Toulouse, Strasbourg, Versailles).

8.2.1. 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 Défis du Numérique which is managed by BPI France, and will be funded thanks to the so-called Plan d'Investissements d'Avenir.

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

[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.

8.3. European Initiatives

- Innovative Training Network POEMA (Polynomial Optimization, Efficiency through Moments and Algebra) - ITN Marie Curie H2020 program.

  `Duration:` 2019–2023

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

  POEMA is part of the Marie Sklodowska-Curie Actions — Innovative Training Networks (ITN) funding scheme.

  POEMA aims 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.

PROSECCO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. 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.

9.1.1.2. AJACS

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

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

Duration: October 2014 - March 2019.

Coordinator: Alan Schmitt, Inria (France)

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.

9.1.1.3. 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.

9.1.1.4. 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 2021

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.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. 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.

9.2.1.2. 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.

9.2.1.3. NEXTLEAP (304)

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

The objective of the NEXTLEAP project is to build the fundamental interdisciplinary internet science necessary to create decentralized, secure, and rights-preserving protocols for the next generation of collective awareness platforms. The long-term goal of NEXTLEAP is to have Europe take the "next leap ahead" of the rest of the world by solving the fundamental challenge of determining how both to scientifically build and how to help citizens and institutions adopt open-source decentralized and privacy-preserving digital social platforms in contrast to proprietary centralized cloud-based services and pervasive surveillance that function at the expense of rights and technological sovereignty.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

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

- 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

9.3.2. Participation in Other International Programs

9.3.2.1. 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.

9.3.2.2. 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

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Éric Tanter (University of Chile) joined Inria as a Visiting Professor from Jul 2018 to March 2019 and from August to December 2019; he gave various seminars at Inria including one entitled "Gradual Parametricity, Revisited";
- Li-yao Xia (University of Pennsylvania) visited Prosecco on 7 January and gave a talk entitled "From C to Interaction Trees";
- Matías Toro (University of Chile) visited Prosecco on 9 January and gave a talk entitled "Type-Driven Gradual Security with References";
- Deepak Garg (MPI-SWS) visited Prosecco on 29 January and 20 November;
- Gilles Barthe (MPI-SP) visited Prosecco on various occasions: 29 January, 3–6 June, 9–13 Sept, and 7–9 October 2019;

- Jeremy Siek (Indiana University) visited Prosecco on 21 February and gave a seminar entitled "Toward Efficient Gradual Typing";
- Andrew Tolmach (Portland State University) visted Prosecco on 8–12 April and gave a seminar on "Enforcing C-level security policies using machine-level tags";
- Guido Martinez (CIFASIS-CONICET Rosario) visited Prosecco on various occasions: April 15–19, ICFP, 30 September to 12 October
- Nikos Vasilakis (University of Pennsylvania) visited Prosecco on 15–19 July and gave a seminar on "Retrofitting Security, Module by Module";
- Clement Pit-Claudel (MPI) visited Prosecco on 14 August;
- Kevin Liao (MPI-SP) visited Prosecco on various occasions and gave a seminar on "ILC: A Calculus for Composable, Computational Cryptography";
- Tahina Ramananandro (Microsoft Research) visited Prosecco on 30 September to 15 October and gave a seminar on "EverParse";
- Nik Swamy (Microsoft Research) and Aymeric Fromherz (CMU) visited Prosecco from 7–11 October and gave a seminar on "Verifying a mixture of C and assembly code with Low* and Vale";
- Jonathan Protzenko (Microsoft Research) visited Prosecco on 30 September to 15 October and gave a seminar on "The EverCrypt verified cryptographic provider";
- Jakob von Raumer (University of Nottingham) visited Prosecco on 23 October and gave a seminar on "Indexed Inductive Types";
- Bas Spitters (COBRA, Aarhus University) visited Prosecco on 25–29 November and gave a seminar on "ConCert: A Smart Contract Certification Framework in Coq";
- Adrien Koutsos (MPI-SP) visited Prosecco on 5 November and gave a talk on "5G-AKA authentication protocol privacy";
- Akram El-Korashy (MPI-SWS) visited Prosecco on 20 November;
- Shin-ya Katsumata (NII, Tokyo, Japan) visited Prosecco on 25–28 November;
- Ian Miers (Johns Hopkins University) visited Prosecco on 29 November and gave a seminar on "Zcash, Blockchains, and the possibilities for formal verification with zero-knowledge";

9.4.1.1. Internships

- Antoine Van Muylder (Paris 7): from April to September 2019 – advised by Catalin Hritcu, Exequiel Rivas, and Kenji Maillard
- Guillaume Gette: from April to September 2019 – advised by Karthikeyan Bhargavan
- Mikhail Volkhov: from April to August 2019 – advised by Karthikeyan Bhargavan and Prasad Naldurg

9.4.2. Visits to International Teams

- Catalin Hritcu visited EPFL Lausanne on 25–27 September;
- Catalin Hritcu, Carmine Abate, Roberto Blanco, and Jeremy Thibault visited MPI-SWS in Saarbrücken on 18–22 October and 1–3 December;
- Catalin Hritcu visited Chalmers University in Gothenburg on 4–6 December;

QUANTIC Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

- **Paris EMERGENCE project ENDURANCE**: In the framework of the Paris Ile de France program “EMERGENCE”, Zaki Leghtas has received a funding for his research program "Multi-photon processes in superconducting circuits for quantum error correction". This grant of 230k euros has allowed us to purchase the experimental equipment to complement the experiment based at ENS.
- **DIM SIRTEQ PhD fellowship**: We have received funding from DIM SIRTEQ to cover half of the PhD of Jérémie Guillaud under supervision of Mazyar Mirrahimi.
- **DIM SIRTEQ project SCOOP**:Half a PhD grant for Marius Villiers, supervised by Zaki Leghtas and Audrey Cottet (ENS Paris). The project is to use quantum circuits to detect the entanglement of a single Cooper pair. University.
- **EDPIF PhD fellowship**: Ecole Doctorale de Physique en Ile de France has funded half a PhD grant for Marius Villiers.
- **DGA PhD fellowship**: Direction Générale de l’Armement has funded half a PhD grant for Camille Berdou supervised by Zaki Leghtas. The project is to build a repetition code of cat-qubits.
- **Mines Paristech PhD Fellowship**: Ecole des Mines Paristech has funded half a PhD grant for Camille Berdou.
- **PSL working group on “structural stability and chaos in open quantum systems”**: This is a Groupe de Travail with researchers from CEREMADE (Paris Dauphine) and Observatoire de Paris under the direction of Jacques Fejoz. In the framework of the PhD thesis of Michiel Burgelman, we study the dynamics of superconducting Josephson circuits driven by strong microwave drives.

7.2. National Initiatives

- **ANR project ENDURANCE**: In the framework of the ANR program “Accueil de chercheur de haut niveau”, Zaki Leghtas has received a funding for his research program "Multi-photon processes in superconducting circuits for quantum error correction". This grant of 400k euros has allowed us to purchase the experimental equipment to build a new experiment based at ENS. The project started in March 2016 for 42 months.
- **ANR project HAMROQS**: In the framework of the ANR program JCJC, Alain Sarlette has received a funding for his research program "High-accuracy model reduction for open quantum systems". This grant of 212k euros started on april 2019 and will run for 4 years.

7.3. European Initiatives

7.3.1. FP7 & H2020 Projects

Program: H2020

Type: ERC

Project acronym: ECLIPSE

Project title: Exotic superconducting CIrcuits to Probe and protect quantum States of light and mattEr

Duration: 2019-

Coordinator: Zaki Leghtas, Mines Paristech

Program: H2020

Type: Quantera

Project acronym: QuCos

Project title: Quantum Computation with Schrödinger cat states

Duration: 2019-

Coordinator: Gerhard Kirchmair, University of Innsbruck, Austria.

Inria contacts: Zaki Leghtas and Mazyar Mirrahimi

Other partners: ENS Lyon (France), Karlsruhe Institut of Technology (Germany), Quantum Machines (Israel), National Institute for Research and Development of Isotopic and Molecular Technologies, Romania.

Abstract: This project seeks to establish a radically new, alternative approach to realizing the fundamental building blocks of quantum computers with superconducting qubits. In the next 3 years, we plan to employ only a handful of realistic components to realize robust error-corrected logical quantum bits. We aim to demonstrate the same level of protection provided by a few hundreds of qubits (with properties beyond the state of the art) in today's mainstream approach of the so-called surface code architecture. Our alternative approach is known as cat codes, because it employs multiple interconnected high coherence cavity modes with non-linear dissipation, to encode a qubit in superpositions of Schrödinger cat states. Our project combines realizing the quantum processor architecture as well as the control system and the protocols that drive it, building towards a full-stack error-corrected quantum computer. The partners in our collaboration form a strong synergetic group that has the full range of expertise needed to design and realize these systems, and to obtain these challenging goals. Furthermore, all partners of our project, including both industry and academia, have worked together and published works in the fields of quantum computing and quantum information processing. We aim to implement error protected qubits, fault tolerant operations, and demonstrate the scalability of this approach by realizing a repetition code. Our project will enable quantum experiments towards the ambitious and well-defined goal of constructing a logical qubit, on which we can perform gates, and most importantly, quantum error-correction (QEC).

7.3.2. Collaborations with Major European Organizations

Partner 1: ENS Lyon

We are pursuing our interdisciplinary work about quantum control from theoretical aspects in direct collaboration with existing experiments (ENS Lyon) with the group of Benjamin Huard, former member of the QUANTIC team. Joint papers are published and underway. The ANR-JCJC project HAMROQS by Alain Sarlette has Benjamin Huard as external supporting collaborator.

Partner 2: Laboratoire Kastler Brossel

We have been continuing collaborations with the teams of Samuel Deleglise and Igor Dotsenko from Laboratoire Kastler Brossel on the theoretical analysis of their experiments.

Partner 3: Ghent University.

Alain Sarlette has been collaborating with applied mathematicians interested in quantum control at UGent in the framework of thesis co-supervisions. One PhD student has successfully defended his thesis this year (Zhifei Zhang).

7.4. International Initiatives

7.4.1. Inria International Labs

Inria@EastCoast
Associate Team involved in the International Lab:

7.4.1.1. TAQUILLA

Title: TAilored QUantum Information protocoLs for quAntum superconducting circuits

International Partner (Institution - Laboratory - Researcher):

Université Yale (United States) -Department of Applied Physics - Michel Devoret

Start year: 2019

See also: https://team.inria.fr/quantic/Taquilla.html

We seek to establish an alternative approach to quantum error correction (QEC) for superconducting qubits. This approach, developed through the Inria-Yale collaboration, is known under the name of cat codes, because it employs multiple interconnected high coherence cavity modes with non-linear dissipation to encode a qubit in superpositions of Schrödinger cat states. We aim to implement error protected qubits, fault tolerant operations, and demonstrate the scalability of this approach. Our project will enable quantum experiments towards the ambitious and well-defined goal of constructing a logical qubit, on which we can perform gates, and most importantly, QEC.

7.4.2. Participation in Other International Programs

- **Yale-ARO subaward:** In the framework of the collaborations with Yale university, Quantic team has received a sub-award of 500k dollars over 4 years starting in 2018 from Yale university. This sub-award is part of an ARO (Army Research Office) grant received by our collaborators at Yale and covers the expenses related to our collaborations (hiring of new PhD students and postdocs at Inria and travels between Inria and Yale).
- **DARPA:** Alain Sarlette is international key personnel on the DARPA project "The Quantum Computing Revolution and Optimization: Challenges and Opportunities" led by optimization researchers at Lehigh Universty. This project of about 2M dollars can fund some exchanges during the coming years.
- **Berkeley exchange initiative:** P. Rouchon and A. Sarlette have set up an exchange initiative with Birgitta Whaley about quantum control and error correction based on continuous measurements. This initiative has funded a research visit of Gerardo Cardona at Berkeley; a student from Berkeley is bound to visit us soon in return.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

P.S. Pereira da Silva (Escola Politecnica, PTC, University of Sao Paulo, Brazil) made two visits (September 16 to 27 and December 2 to 6) to investigate with Pierre Rouchon motion planning issues based on Lyapunov tracking for quantum gate generations for open quantum systems governed by Lindblad master equations.

7.5.2. Visits to International Teams

7.5.2.1. Research Stays Abroad

- In the framework of our collaborations with Yale (Taquilla associated team), Mazyar Mirrahimi and Michiel Burgelman have spent 3 months at Yale. In the same framework Philippe Campagne-Ibarcq and Christian Siegele also made a visit of 5 days during the same period.
- In the framework of the Berkeley exchange initiative, Gerardo Cardona has spent a month (October 2019) in the research group of Birgitta Whaley at Berkeley University.

REO Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

Irene Vignon Clementel is a member of the project iLite (09/16-10/21), RHU-santé grant, a large French hospital-medical research consortium that aims at developing innovations for liver and tissue engineering (Inria PI: Dirk Drasdo).

8.1.2. APHP-Inria collaboration

Participants: Nour Bou Saleh, Quentin Nicolas, Nicolas Golse, Irene Vignon-Clementel [local coordinator].

Collaboration with Eric Vibert (APHP - Inserm U1193) for cosupervision of surgery interns (N. Bousaleh, D. Dousse) and engineering intern (Q Nicolas) in the context of the APHP-Inria PhD of N. Golse, on liver modeling and ICG fluorescence.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, Except FP7 & H2020

SimInhale COST Action MP1404, a pan-European network of experts in the field of inhaled medicine, coordinated by Prof. Stavros Kassinos, end: 2019 (http://www.siminhale-cost.eu).

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

Collaboration with :

- Prof. Pal Dag Line from U. of Oslo, Oslo hospital U. with E. Vibert (APHP, Inserm) - N. Golse, I. Vignon-Clementel
- CHUM Centre Hospitalier de l'Université de Montreal (G Soulez and colleagues) - F. Joly (Inria), I. Vignon-Clementel

RITS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. VALET

Title: Redistribution automatique d'une flotte de véhicules en partage et valet de parking

Instrument: ANR

Duration: January 2016 - September 2019

Coordinator: Fawzi Nashashibi

Partners: Inria, Ecole Centrale de Nantes (IRCCyN), AKKA Technologies

Inria contact: Fawzi Nashashibi

Abstract: The VALET project proposes a novel approach for solving car-sharing vehicles redistribution problem using vehicle platoons guided by professional drivers. An optimal routing algorithm is in charge of defining platoons drivers' routes to the parking areas where the followers are parked in a complete automated mode. The main idea of VALET is to retrieve vehicles parked randomly on the urban parking network by users. These parking spaces may be in electric charging stations, parking for car sharing vehicles or in regular parking places. Once the vehicles are collected and guided in a platooning mode, the objective is then to guide them to their allocated parking area or to their respective parking lots. Then each vehicle is assigned a parking place into which it has to park in an automated mode.

8.1.1.2. Hianic

Title: navigation autonome dans les foules inspirée par les humains (Human Inspired Autonomous Navigation In Crowds)

Instrument: ANR

Duration: January 2018 - December 2020

Coordinator: Anne Spalanzani (Inria Rhône-Alpes, Chroma research team)

Partners: Inria Rhône-Alpes, Inria Paris, LIG Laboratoire d'Informatique de Grenoble, LS2N - ECN Laboratoire des Sciences du Numérique de Nantes

Inria contact: Fawzi Nashashibi

Abstract: The HIANIC project will try to address some problems that will arise when these cars are mixed with pedestrians. The HIANIC project will develop new technologies in term of autonomous navigation in dense and human populated traffic. It will explore the complex problem of navigating autonomously in shared-space environments, where pedestrians and cars share the same environment.

Such a system will contribute both to urban safety and intelligent mobility in "shared spaces". Negotiation will help to avoid frozen situations increasing the vehicle's reactivity and optimizing the navigable space. Negotiation, Human-Aware Navigation and Communication will contribute to a better public acceptance of such autonomous systems and facilitate their penetration in the transportation landscape.

8.1.2. FUI

8.1.2.1. PAC V2X

Title: Perception augmentée par coopération véhicule avec l'infrastructure routière

Instrument: FUI

Duration: September 2016 - May 2020

Coordinator: SIGNATURE Group (SVMS)

Partners: DigiMobee, LOGIROAD, MABEN PRODUCTS, SANEF, SVMS, VICI, Inria, VEDECOM

Inria contact: Raoul de Charette

Abstract: The objective of the project is to integrate two technologies currently being deployed in order to significantly increase the time for an automated vehicle to evolve autonomously on European road networks. It is the integration of technologies for the detection of fixed and mobile objects such as radars, lidars, cameras ... etc. And local telecommunication technologies for the development of ad hoc local networks as used in cooperative systems.

8.1.3. Competitivity Clusters

RITS team is a very active partner in the competitivity clusters, especially MOV'EO and System@tic. We are involved in several technical committees like the DAS SUR of MOV'EO for example.
RITS is also the main Inria contributor in the VEDECOM institute (IEED).

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. AUTOCITS

Title: AUTOCITS Regulation Study for Interoperability in the Adoption of Autonomous Driving in European Urban Nodes

Program: CEF- TRANSPORT Atlantic corridor

Duration: November 2016 - March 2019

Coordinator: Indra Sistemas S.A. (Spain)

Partners: Indra Sistemas S.A. (Spain); Universidad Politécnica de Madrid (UPM), Spain; Dirección General de Tráfico (DGT), Spain; Inria (France); Instituto Pedro Nunes (IPN), Portugal; Autoridade Nacional de Segurança Rodoviária (ANSR), Portugal; Universidade de Coimbra (UC), Portugal.

Inria contact: Fawzi Nashashibi, Mohammad Abualhoul

Abstract: The aim of the Study is to contribute to the deployment of C-ITS in Europe by enhancing interoperability for autonomous vehicles as well as to boost the role of C-ITS as catalyst for the implementation of autonomous driving. Pilots will be implemented in 3 major Core Urban nodes (Paris, Madrid, Lisbon) located along the Core network Atlantic Corridor in 3 different Member States. The Action consists of Analysis and design, Pilots deployment and assessment, Dissemination and communication as well as Project Management and Coordination.

8.2.2. Collaborations with Major European Organizations

RITS is member of the **euRobotics AISBL** (Association Internationale Sans But Lucratif) and the Leader of "People transport" Topic. This makes from Inria one of the rare French robotics representatives at the European level. See also: http://www.eu-robotics.net/

RITS is a full partner of **VRA – Vehicle and Road Automation**, a support action funded by the European Union to create a collaboration network of experts and stakeholders working on deployment of automated vehicles and its related infrastructure. VRA project is considered as the cooperation interface between EC funded projects, international relations and national activities on the topic of vehicle and road automation. It is financed by the European Commission DG CONNECT and coordinated by ERTICO – ITS Europe. See also: http://vra-net.eu/

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

RITS has signed 3 MoU with the following international laboratories:

- Vehicle Dynamics and Control Laboratory, Seoul National University (SNU), S. Korea: international cooperation agreement for Graduate-Level Academic and Research Collaboration
- MICA Lab, Hanoi University of Science and Technology, Vietnam: cooperation agreement for research collaboration and PhD students co-supervision
- Integrated Industrial Design Lab (INDEL) of the Department of Product and Systems Design Engineering, University of the Aegean, Greece: international cooperation agreement for Graduate-Level Academic and Research Collaboration

8.3.2. Participation in Other International Programs

Samuel de Champlain Québec-France collaboration program: "Vision par ordinateur en conditions difficiles", cooperation between Raoul de Charette and Jean-François Lalonde from Laval University.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Plamen Petrov from Technical University of Sofia, from July to September 2019.

8.4.1.1. Internships

- Pranav Agarwal, from August 2019.
- Fares Bessam, Master student, April-September 2019.
- Manuel Gonzalez and Leonardo Ward, from Simon Bolivar University, Venezuela, from September 2019.
- Manohar KV, May-July 2019.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Maximilian Jaritz was at UC San Diego, visiting SU Lab directed by Hao Su, from October 1st 2018 to February 15th 2019.

SECRET Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR DEREC** (10/16 → 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 → 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 → 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. 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.

8.2.1.2. 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.

8.2.1.3. H2020 FET Flagship on Quantum Technologies - CiViQ

Title: CiViQ *Continuous Variable Quantum Communications*

Program: H2020 FET Flagship on Quantum Technologies

Duration: October 2018 - September 2021

PI: Anthony Leverrier

The goal of the CiViQ project is to open a radically novel avenue towards flexible and cost-effective integration of quantum communication technologies, and in particular Continuous-Variable QKD, into emerging optical telecom- munication networks. CiViQ aims at a broad technological impact based on a systematic analysis of telecom-defined user-requirements. To this end CiViQ unites for the first time a broad interdisciplinary community of 21 partners with unique breadth of experience, involving major telecoms, integrators and developers of QKD. The work targets advancing both the QKD technology itself and the emerging "software network" approach to lay the foundations of future seamless integration of both. CiViQ will culminate in a validation in true telecom network environment. Project-specific network integration and software development work will empower QKD to be used as a physical-layer-anchor securing critical infrastruc- tures, with demonstration in QKD-extended software-defined networks.

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 - 2019

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.
- NTT Secure Platforms Laboratories (Japan): quantum cryptanalysis, symmetric cryptography.
- University of Sherbrooke (Canada): quantum codes.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Thomas Peyrin, NTU Singapore, January 2019 and July 2019
- Mustafa Mahmoud Mohammed Kairallah, NTU Singapore, July 2019
- Léo Ducas, CWI Amsterdam, NL, March 2019
- Akinori Hosoyamada, NTT Secure Platform Labaratories, Tokyo, Japan, March 2019 and November 2019
- Yu Sasaki, NTT Secure Platform Labaratories, Tokyo, Japan, November 2019
- Gregor Leander, Ruhr Université Bochum, Germany, November 2019

8.4.1.1. Internships

- Pierre Briaud, MPRI, March-Aug. 2019
- Lucien Grouès, Telecom ParisTech, March-Sept. 2019
- Antonio Florez Gutierrez, Université Paris Saclay, March-Aug. 2019
- Sohaïb Ouzineb, Telecom ParisTech, July-Aug. 2019
- Elodie Rohart-Barbey, INSA Rouen, June-Aug. 2019
- Augustin Bariant, Ecole Polytechnique, April-Aug. 2019

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- Bar-Ilan Unversity, Israel, June 16-18, invitation by Nathan Keller (A. Canteaut and G. Leurent)
- Rostock University, Rostock, Germany, June 23-28, invitation to the Institut für Mathematik by Gohar Kyureghyan, (L. Perrin).
- NTT, Tokyo, Japan, August 27-September 27, invitation by Yu Sasaki (F. Sibleyras)

SERENA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

MILC (DMI RFSI, 2018–2019): "Mesure et Intégrale de Lebesgue en Coq", with LIPN (Université de Paris 13), and TOCCATA (Inria Saclay - Île-de-France). SERENA representants are François Clément and Vincent Martin (UTC).

GiS: scientific collaboration network between ten public institutions from the Paris (Ile-de-France) region, focused on natural resources and environment. The project-team SERENA is a member.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- ERC GATIPOR: "Guaranteed fully adaptive algorithms with tailored inexact solvers for complex porous media flows". The subject of this consolidator grant are new approaches to porous media multiphase flows: inexact Newton-multigrid solvers, local stopping criteria, adaptivity, and a posteriori error control. The goal is to guarantee the overall simulation error and to speed-up importantly the present-day simulations. SERENA representant is M. Vohralík (grant leader, 75% commitment), period 2015–2020.
- ERC EMC2: " Extreme-scale Mathematically-based Computational Chemistry". The goal of this project is to develop physical and chemical models in chemistry, condensed matter physics, molecular biology, materials science, and nanosciences, altogether with mathematically-certified and numerically-efficient algorithms, and to implement them in a scalable way on various computer architectures. There are 4 principal investigators and a little more than 10 co-investigators. SERENA representant is M. Vohralík (co-investigator, 10% commitment), period 2019–2025.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

Erik Burman, Professor, University College London, unfitted methods.

Ulrich Rüde, Professor, University of Erlangen-Nürnberg, multigrid methods.

Iain Smears, Lecturer, University College London, local-global approximations.

Benjamin Stamm, Professor, RTWH Aachen University, eigenvalue problems (first-principle molecular simulation).

Barbara Wohlmuth, professor, Technical University Munich, multigrid methods.

9.3.2. Participation in Other International Programs

9.3.2.1. Inria International Chairs

IIC GUERMOND Jean-Luc

Title: Curved H(div), H(curl) elements, and magnetohydrodynamics & Approximation of hyperbolic systems

International Partner (Institution - Laboratory - Researcher):

Texas A&M University (United States) - Department of Mathematics - Jean-Luc Guermond

Duration: 2019 - 2023

Start year: 2019

See also: https://www.math.tamu.edu/~guermond/

The program is articulated around two themes: (1) Theoretical aspects in finite elements and applications to multi-physics magneto-hydrodynamics; (2) Finite element approximation of hyperbolic systems and applications. The results from this research will have applications in problems related to porous media flows, magnetohydrodynamics, water management, and compressible and incompressible fluid flows.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Hend Ben Ameur, Professor at IPEST and member of ENIT-Lamsin, Tunis, Tunisia, November 4–15.

Gregor Gantner, Vienna University of Technology. Collaboration on IGA methods. September 23–27.

Thirupathi Gudi, Indian Institute of Science, Bangalore. Collaboration on local-global approximations. June 10–17.

Dirk Praetorius, Vienna University of Technology. Collaboration on cost-optimality of fully adaptive algorithms. March 21–23.

Ivan Yotov, Professor, University of Pittsburgh. Inria Paris invited professor, September 1–December 15, 2019. Collaboration on multilevel and space-time domain decomposition methods.

9.4.1.1. Internships

Théo Kaprélian, internship at Ecole Centrale de Lyon, from September 2019 to February 2020, supervised by Martin Vohralík.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

+ Géraldine Pichot was invited for a one week stay at Pennstate University, USA for a collaboration with Pr. Ludmil Zikatanov.
+ Géraldine Pichot was invited for a one week stay at University of Bergen, Norway for a collaboration with Pr. Florin Radu.

SIERRA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

Alexandre d'Aspremont: IRIS, PSL "Science des données, données de la science".

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

ERC Sequoia Title: Robust algorithms for learning from modern data

Programm: H2020

Type: ERC

Duration: 2017-2022

Coordinator: Inria

Inria contact: Francis Bach

Abstract: Machine learning is needed and used everywhere, from science to industry, with a growing impact on many disciplines. While first successes were due at least in part to simple supervised learning algorithms used primarily as black boxes on medium-scale problems, modern data pose new challenges. Scalability is an important issue of course: with large amounts of data, many current problems far exceed the capabilities of existing algorithms despite sophisticated computing architectures. But beyond this, the core classical model of supervised machine learning, with the usual assumptions of independent and identically distributed data, or well-defined features, outputs and loss functions, has reached its theoretical and practical limits. Given this new setting, existing optimization-based algorithms are not adapted. The main objective of this project is to push the frontiers of supervised machine learning, in terms of (a) scalability to data with massive numbers of observations, features, and tasks, (b) adaptability to modern computing environments, in particular for parallel and distributed processing, (c) provable adaptivity and robustness to problem and hardware specifications, and (d) robustness to non-convexities inherent in machine learning problems. To achieve the expected breakthroughs, we will design a novel generation of learning algorithms amenable to a tight convergence analysis with realistic assumptions and efficient implementations. They will help transition machine learning algorithms towards the same widespread robust use as numerical linear algebra libraries. Outcomes of the research described in this proposal will include algorithms that come with strong convergence guarantees and are well-tested on real-life benchmarks coming from computer vision, bioinformatics, audio processing and natural language processing. For both distributed and non-distributed settings, we will release open-source software, adapted to widely available computing platforms.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Sebastian Pokutta from TU & Zuse Institute, Berlin, December 2019.
- Critobal Guzman from Universidad Católica de Chile, July 2019.
- Quentin Berthet from University of Cambridge, from Feb 2019 until Apr 2019.
- Eduard Gorbunov from Moscow Institute of Physics and Technology, Oct 2019.
- Song Mei, from Stanford University, from Sep 2019 until Oct 2019.
- Anant Raj, from M.P.I. Tubingen, from Oct 2019.
- Aadirupa Saha, from Indian Institute of Technology, Bangalore, from Nov 2019

VALDA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

The ISORE project from the Île-de-France region (6k€ grant, DIM RFSI), which started in 2019, was completed in 2020.

Leonid Libkin received funding from FSMP through his *Chaire d'Excellence*, in the fall of 2019.

Pierre Senellart is a recipient of a Chair of the PaRis Artificial Intelligence Research InstitutE, PRAIRIE, sarting in the fall of 2019.

9.2. National Initiatives

9.2.1. ANR

Valda has been part of four ANR projects in 2019:

HEADWORK (2016–2021; 38 k€ for Valda, budget managed by Inria), together with IRISA (Druid, coordinator), Inria Lille (Links & Spirals), and Inria Rennes (Sumo), and two application partners: MNHN (Cesco) and FouleFactory. The topic is workflows for crowdsourcing. See http://headwork.gforge.inria.fr/.

BioQOP (2017–2020; 66 k€ for Valda, budget managed by ENS), with Idemia (coordinator) and GREYC, on the optimization of queries for privacy-aware biometric data management. See http://bioqop.di.ens.fr/.

CQFD (2018–2022; 19 k€ for Valda, budget managed by Inria), with Inria Sophia (GraphIK, coordinator), LaBRI, LIG, Inria Saclay (Cedar), IRISA, Inria Lille (Spirals), and Télécom ParisTech, on complex ontological queries over federated and heterogeneous data. See http://www.lirmm.fr/cqfd/.

QUID (2018–2022; 49 k€ for Valda, budget managed by Inria), LIGM (coordinator), IRIF, and LaBRI, on incomplete and inconsistent data. See https://quid.labri.fr/home.html.

Camille Bourgaux is participating in the AI Chair of Meghyn Bienvenu on *INTENDED (Intelligent handling of imperfect data)* to start in 2020.

9.3. European Initiatives

9.3.1. Collaborations in European Programs, Except FP7 & H2020

A bilateral French–German ANR project, entitled *EQUUS – Efficient Query answering Under UpdateS* was accepted in 2019. It will start in 2020. It involves CNRS (CRIL, CRIStAL, IMJ), Télécom Paris, HU Berlin, and Bayreuth University, in addition to Inria Valda.

9.4. International Initiatives

9.4.1. Informal International Partners

Valda has strong collaborations with the following international groups:

Univ. Edinburgh, United Kingdom: Paolo Guagliardo, Andreas Pieris

Univ. Oxford, United Kingdom: Michael Benedikt, Dan Olteanu, and Georg Gottlob

TU Dresden, Germany: Markus Krötzsch and Sebastian Rudolph

Dortmund University, Germany: Thomas Schwentick

Free Univ. Bozen-Bolzano, Italy: Ana Ozaki

Warsaw University, Poland: Mikołaj Bojańczyk and Szymon Toruńczyk

Tel Aviv University, Israel: Daniel Deutch and Tova Milo

Drexel University, USA: Julia Stoyanovich

Univ. California San Diego, USA: Victor Vianu

Pontifical Catholic University of Chile: Marcelo Arenas, Pablo Barceló

National University of Singapore: Stéphane Bressan

9.5. International Research Visitors

9.5.1. Visits of International Scientists

Victor Vianu, Professor at UC San Diego and former holder of an Inria international chair, spent 6 months within Valda, as a University Paris-Diderot and ENS invited professor.

Thomas Schwentick, Professor at TU Dortmund, spend 1 month within Valda in May–June.

WHISPER Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

- City of Paris, 2016-2019, 100 000 euros. As part of the "Émergence - young team" program the city of Paris is supporting part of our work on domain-specific languages and trustworthy domain-specific compilers.

9.2. National Initiatives

9.2.1. ANR

ITrans - awarded in 2016, duration 2017 - 2020

Members: LIP6 (Whisper), David Lo (Singapore Management University)

Coordinator: Julia Lawall

Whisper members: Julia Lawall, Gilles Muller, Lucas Serrano, Van-Anh Nguyen

Funding: ANR PRCI, 287,820 euros.

Objectives:

Large, real-world software must continually change, to keep up with evolving requirements, fix bugs, and improve performance, maintainability, and security. This rate of change can pose difficulties for clients, whose code cannot always evolve at the same rate. This project will target the problems of *forward porting*, where one software component has to catch up to a code base with which it needs to interact, and *back porting*, in which it is desired to use a more modern component in a context where it is necessary to continue to use a legacy code base, focusing on the context of Linux device drivers. In this project, we will take a *history-guided source-code transformation-based* approach, which automatically traverses the history of the changes made to a software system, to find where changes in the code to be ported are required, gathers examples of the required changes, and generates change rules to incrementally back port or forward port the code. Our approach will be a success if it is able to automatically back and forward port a large number of drivers for the Linux operating system to various earlier and later versions of the Linux kernel with high accuracy while requiring minimal developer effort. This objective is not achievable by existing techniques.

VeriAmos - awarded in 2018, duration 2018 - 2021

Members: Inria (Antique, Whisper), UGA (Erods)

Coordinator: Xavier Rival

Whisper members: Julia Lawall, Gilles Muller

Funding: ANR, 121,739 euros.

Objectives:

General-purpose Operating Systems, such as Linux, are increasingly used to support high-level functionalities in the safety-critical embedded systems industry with usage in automotive, medical and cyber-physical systems. However, it is well known that general purpose OSes suffer from bugs. In the embedded systems context, bugs may have critical consequences, even affecting human life. Recently, some major advances have been done in verifying OS kernels, mostly employing interactive theorem-proving techniques. These works rely on the formalization of the programming language semantics, and of the implementation of a software component, but require significant human intervention to supply the main proof arguments. The VeriAmos project will attack this problem by building on recent advances in the design of domain-specific languages and static

analyzers for systems code. We will investigate whether the restricted expressiveness and the higher level of abstraction provided by the use of a DSL will make it possible to design static analyzers that can statically and fully automatically verify important classes of semantic properties on OS code, while retaining adequate performance of the OS service. As a specific use-case, the project will target I/O scheduling components.

9.3. International Initiatives

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

9.3.1.1. CSG

Title: Proving Concurrent Multi-Core Operating Systems

International Partner (Institution - Laboratory - Researcher):

University of Sydney (Australia) - Willy Zwaenepoel

Start year: 2019

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

The initial topic of this cooperation is the development of proved multicore schedulers. Over the last two years, we have explored a novel approach based on the identification of key scheduling abstractions and the realization of these abstractions as a Domain-Specific Language (DSL), Ipanema. We have introduced a concurrency model that relies on execution of scheduling events in mutual execution locally on a core, but that still permits reading the state of other cores without requiring locks.

In the three next years, we will leverage on our existing results towards the following directions: (i) Better understanding of what should be the best scheduler for a given multicore application, (ii) Proving the correctness of the C code generated from the DSL policy and of the Ipanema abstract machine, (iii) Extend the Ipanema DSL to the domain of I/O request scheduling, (iv) Design of a provable complete concurrent kernel.

9.3.2. Inria International Partners

9.3.2.1. Informal International Partners

Julia Lawall and Gilles Muller collaborate with David Lo and Lingxiao Jiang of Singapore Management University in the context of the ANR-NRF funded project ITrans. This project supports the PhD of Lucas Serrano. In 2019, this collaboration led to an experience paper at ECOOP on a transformation tool (a variant of Coccinelle) for Java [21] and a tool paper at ICSE on using machine learning for identifying bug-fixing patches for the Linux kernel [19]. The latter has been extended to a journal article published in the IEEE Transactions on Software Engineering [11]. Lawall and Serrano spent two weeks visiting Lo and Jiang at Singapore Management University in December 2019.

Julia Lawall collaborates with Jia-Ju Bai at Tsinghua University on bug finding for the Linux kernel. In 2019, this collaboration led to a paper at SANER on detecting data races in device drivers [17], a paper at ISSRE on extending Linux kernel fuzzing to be able to detect bugs in error-handling code [20], a paper at ASPLOS on detection of unnecessary spinning in the Linux kernel [14], a paper at USENIX ATC on detection of use-after free concurrency bugs in the Linux kernel [13]. Bai visited the Whisper team for 2 months starting in January 2019. Lawall visited Bai at Tsinghua University for one week in August.

Michele Martone of the Leibniz Supercomputing Centre in Munich, Germany has been using Coccinelle in an HPC context and giving workshops on Coccinelle in the HPC research engineer community. Martone has contributed some patches to Coccinelle and we keep in touch with him about possible improvements to Coccinelle that may have an impact on its use in the HPC community.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Jia-Ju Bai visited the Whisper team for 2 months starting in January 2019. During this time, he and Julia Lawall worked on a prototype of an interprocedural program analysis tool for C code.

Victor Miraldo (Ultrech University) visited the Whisper team for 2 weeks in June 2019, where he worked with Pierre-Évariste Dagand on data structures for efficient differencing of data structures.

9.4.1.1. Internships

Pierre-Évariste Dagand has supervised the Master 2 research internship of Pierre Nigron (University Paris Diderot), from April to August 2019, on the topic of "Effectful programs and their proofs in a dependently-typed setting". Pierre Nigron was awarded a DGA-Inria grant to pursue a PhD under Julia Lawall's supervision, co-supervised by Pierre-Évariste Dagand.

Pierre-Évariste Dagand has supervised the Bachelor research internship of Quentin Corradi (École Normale Supérieure de Lyon), for 6 weeks starting in June 2019, on the topic of "A Formal Semantics of SIMD Instruction Sets".

Pierre-Évariste Dagand has supervised a pre-doctoral internship of Rémi Oudin (École Normale Supérieure de Cachan), from April to August 2019, on the topic of "Hardware interfaces for transiently-powered systems". Rémi Oudin was awarded a "Contrat Doctoral Spécifique pour Normaliens".

9.4.2. Visits to International Teams

Gilles Muller spent two weeks in November 2019 visiting the University of Sydney as part of our associated team.

Julia Lawall spent one week at Tsinghua University visiting the group of Jia-Ju Bai in August 2019. Julia Lawall and Lucas Serrano spent two weeks at Singapore Management University visiting the group of David Lo and Lingxiao Jiang in December 2019. During the latter visit, Lawall and Serrano also visited National University of Singapore and Lawall also visited Yale-NUS.

WILLOW Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. PRAIRIE

Participants: Ivan Laptev, Jean-Paul Laumond, Jean Ponce, Josef Sivic.

The Prairie Institute (PaRis AI Research InstitutE) is one of the four French Institutes for Interdisciplinary Artificial Intelligence Research (3IA), which were created as part of the national French initiative on AI announced by President Emmanuel Macron on May 29, 2018. It brings together five academic partners (CNRS, Inria, Institut Pasteur, PSL University, and University of Paris) as well as 17 industrial partners, large corporations which are major players in AI at the French, European and international levels, as well as 45 Chair holders, including four of the members of WILLOW (Laumond, Laptev, Ponce, Sivic). Ponce is the scientific director of PRAIRIE.

9.1.2. DGA - RAPID project DRAAF

Participant: Ivan Laptev.

DGA DRAAF is a two-year collaborative effort with University of Caen (F. Jurie) and the industrial partner EVITECH (P. Bernas) focused on modelling and recognition of violent behaviour in surveillance videos. The project aims to develop image recognition models and algorithms to automatically detect weapons, gestures and actions using recent advances in computer vision and deep learning to provide an affordable real-time solution reducing effects of threats in public places.

9.2. European Initiatives

9.2.1. IMPACT: Intelligent machine perception

Participants: Josef Sivic, Jean Ponce, Ivan Laptev.

IMPACT is a 5-year collaborative project with Czech Technical University, Center for Robotics, Informatics and Cybernetics (CIIRC) (2017-2022). The IMPACT project focuses on fundamental and applied research in computer vision, machine learning and robotics to develop machines that learn to perceive, reason, navigate and interact with complex dynamic environments. For example, people easily learn how to change a flat tire of a car or perform resuscitation by observing other people doing the same task. This involves advanced visual intelligence abilities such as interpreting sequences of human actions that manipulate objects to achieve a specific task. Currently, however, there is no artificial system with a similar level of cognitive visual competence. Breakthrough progress in intelligent machine perception will have profound implications on our everyday lives as well as science and commerce, with smart assistive robots that automatically learn new skills from the Internet, safer cars that autonomously navigate in difficult changing conditions, or intelligent glasses that help people navigate never seen before environments.

9.3. International Initiatives

9.3.1. Associate team GAYA

Participants: Jean Ponce, Matthew Trager.

GAYA is a joint research team bringing together two Inria project-teams (Thoth, Grenoble and WILLOW, Paris) and Carnegie Mellon University, USA. It focuses on two research themes: (i) semantic structured interpretation of videos, and (ii) studying the geometric properties of object shapes to enhance state-of-the-art object recognition approaches.

Interpreting videos semantically in a general setting, involving various types of video content like home video clips, news broadcasts, feature films, which contain a lot of clutter, non-rigid motion, many "actors" performing actions, person-object and person-person interactions, varying viewpoints, is challenging. This task is being examined increasingly over the past decade, with the availability of large video resources, e.g., YouTube. Despite this progress, an effective video representation for recognizing actions is still missing. To address this critical challenge, we propose a joint optimization framework, wherein we learn the video representation and also develop models for action recognition. Specifically, we aim to exploit the spatio-temporal relations among pixels in a video through graphical models and novel deep learning feature representations.

The second research theme explores geometric aspects of computer vision, in particular how to model three-dimensional objects from their two-dimensional projections, and how the appearance of these objects evolves with changes in viewpoint. Beyond its theoretical interest, this work is critical for developing object recognition algorithms that take into account the three-dimensional nature of the visual world and go beyond the template-matching approaches dominant today. Duality is an important concept in this area, and we are investigating its application to the construction of visual hulls as well as the characterization of the topology of image contours using the Gauss map. Existing results are essentially limited to the Euclidean setting, and we are investigating their generalization to the general projective case.

Partners: CMU (Deva Ramanan, Martial Hebert, Abhinav Gupta, Gunnar Sigurdsson), Inria Thoth (Cordelia Schmid, Karteek Alahari, Pavel Tokmakov).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Pierre-Yves Masse (post-doc, Czech Technical University) spent 50% of his time at Sierra (F. Bach) and Willow teams as a visiting post-doc within the framework of collaboration with the Intelligent Machine Perception project lead by J. Sivic at the Czech Technical University in Prague.
- Vladimir Petrik spent October - Janurary 2020 in Willow as a visiting post-doc within the framework of collaboration with the Intelligent Machine Perception project.
- Mircea Cimpoi spent three weeks in March 2019 in Willow as a visiting post-doc within the framework of collaboration with the Intelligent Machine Perception project.

9.4.1.1. Internships

- Anna Kukleva (Master student, University of Bonn) spent six months in the Willow team working on her Master project under supervision of M. Tapaswi and I. Laptev.

9.4.2. Visits to International Teams

9.4.2.1. Explorer programme

- J.Ponce, multiple visits to CMU's Robotics Institute within the framework of the Gaia associated team