RESEARCH CENTER
Paris

FIELD

Activity Report 2018

Section Partnerships and Cooperations

Edition: 2019-03-07

ALMAnaCH Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. 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.

8.1.2. Competitivity Clusters

- **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]).

8.1.3. Other National Initiatives

- **LECTAUREP project** (2017-2018): An explorative 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 digitized 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**: 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.

8.2. European Initiatives

8.2.1. 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.

8.2.2. 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

8.2.3. Collaborations with Major European Organizations

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

- Universität Zürich, Switzerland (Géraldine Walther) [computational morphology, lexicons]
- 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]
- University of Cambridge, United Kingdom (Ekaterina Kochmar) [text simplification]
- Univerza v Ljubljani [University of Ljubljana], Ljubljana, Slovenia (Darja Fišer) [wordnet development]

8.3. International Initiatives

8.3.1. Participation in International Programs

PHC Maimonide (2018-2019, PI Djamé Seddah, co-PI Yoav Goldberg (Bar Ilan University)). Topics: Building NLP resources for analyzing reactions to major events in Hebrew and French social media.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Dr. Ekaterina Kochmar (University of Cambridge), 3 days in June
- Dr. Teresa Lynn (Dublin City University), 2 stays of 1 week each.

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 - September 2020

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.

9.3. 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.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

- J. Demmel, UC Berkeley, USA
- R. Hipmair, ETH Zurich
- M. Grote, Université de Bâle, Suisse
- F. Assous, Israel

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- Visit to Xavier Claeys of Jan Zapletal from IT4Innovation of University of Ostrava, Czech Republic from 4th to 30th of March 2018. The main topic of the visit was discussions around HPC implementation of multi-trace formulations in the BEM code of IT4Innovation.
- Visit to Laura Grigori of Agnieszka Miedlar, University of Kansas, from Jun 2018 until Jul 2018.
- Visit to Laura Grigori of Qiang Niu, Xi'an Jiaotong Liverpool University, from May 2018 until Jul 2018.
- Visit to Frédéric Nataf of Lawrence Mitchell from University of Durham (UK) from December 17th to 22nd. The main topic of the visit was to finalize the interface of the finite element software Firedrake to our library geneo4PETSc.
- Visit to Frédéric Hecht of T. Chacon of Differential equations and numerical analysis at University of Seville Rectorate form April 23th to May 4th.
- Visit to Frédéric Hecht of P. Degond of Department of Mathematics at Imperial College London form Juin 6th to 10th.

9.5.1.1. Internships

- Visit to Xavier Claeys of Michal Kravchenko from IT4Innovation of University of Ostrava, Czech Republic from 1st of October to 28th of December 2018. The main subject of the visit was effective implementation of multi-trace formulations in the BEM code of IT4Innovation.

9.5.2. Visits to International Teams

9.5.2.1. Research Stays Abroad

- Visit of Xavier Claeys to Ralf Hiptmair at ETH Zuerich from the 19th of August to 25th of August 2018. The main subject of the visit was discussion on boundary integral equations adapted to low frequency electromagnetics.
- Visit of Xavier Claeys to Paul Escapil-Inchauspe at Pontificia Universidad Catholica at Santiago Chile for further collaboration around analysis of local multi-trace formulation for electromagnetics.
- Visit of Laura Grigori to the group of Professor J. Demmel, UC Berkeley, for 6 weeks in July and August 2018.

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.

CMean 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. CNRS Mocha (2017-2018)

Participant: Martin Parisot.

CNRS project call: LEFE

Project acronym: MOCHA

Project title: Multi-dimensiOnal Coupling in Hydraulics and data Assimilation

Coordinator: Martin Parisot

Funding: 14k euros

In collaboration with S. Barthélémy, N. Goutal, S. Ricci, M. Hoang Le.

Multi-dimensionnal coupling in river hydrodynamics offers a conveninent solution to properly model complex flow while limiting the computational cost and making the most of pre-exsiting models. The project aims to adapt the lateral interface coupling proposed in [35] to the implicit version and test it on real data for the Garonne River.

9.1.7. Inria Project Lab "Algae in Silico" (2015-2018)

Participants: Marie-Odile Bristeau, Yohan Penel, Jacques Sainte-Marie, Fabien Souillé.

In the aftermath of the ADT In@lgae (2013–2015), we developed a simulation tool for microalgae culture. An Inria Project Lab "Algae in Silico" has started in collaboration with Inria teams BIOCORE and DYLISS. It concerns microalgae culture for biofuel production and the aim is to provide an integrated platform for numerical simulation "from genes to industrial processes".

9.1.8. Inria Project Lab "CityLab" (2015-2018)

Participants: Vivien Mallet, Raphaël Ventura.

CityLab@Inria studies ICT solutions toward smart cities that promote both social and environmental sustainability.

9.1.9. 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.

9.1.10. 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).

9.1.11. 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.

9.1.12. 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

9.1.13. 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)

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ERC Consolidator Grant (2013-2018)

Participants: Anne Mangeney, Hugo Martin.

The project SLIDEQUAKES is about detection and understanding of landslides by observing and modelling gravitational flows and generated earthquakes and is funded by the European Research Council (2 million euros). More precisely, it deals with the mathematical, numerical and experimental modelling of gravitational flows and generated seismic waves coupled with field measurements to better understand and predict these natural hazards and their link with volcanic, seismic and climatic activities.

9.2.1.2. EoCoE (2015-2018)

Participant: Vivien Mallet.

Title: Energy oriented Centre of Excellence for computer applications
Program: H2020
Duration: October 2015 - October 2018
Coordinator: Édouard Audit (CEA)
Partners: CEA (Commissariat à l'Énergie Atomique et aux Énergies Alternatives, France), Forschungszentrum Julich (Germany), Max Planck Gesellschaft (Germany), ENEA (Agenzia Nazionale Per le Nuove Tecnologie, l'energia E Lo Sviluppo Economico Sostenibile, Italy), CERFACS (European Centre for Research and Advanced Training in Scientific Computing, France), Instytut Chemii Bioorganicznej Polskiej Akademii Nauk (Poland), Universita Degli Studi di Trento (Italy), Fraunhofer Gesellschaft (Germany), University of Bath (United Kingdom), CYL (The Cyprus Institute, Cyprus), CNR (National Research Council of Italy), Université Libre de Bruxelles (Belgium), BSC (Centro Nacional de Supercomputacion, Spain)
Inria contact: Michel Kern (Serena team)
Abstract: The aim of the projevt is to establish an Energy Oriented Centre of Excellence for computing applications (EoCoE). EoCoE (pronounce "Echo") will use the prodigious potential offered by the ever-growing computing infrastructure to foster and accelerate the European transition to a reliable and low carbon energy supply. To achieve this goal, we believe that the present revolution in hardware technology calls for a similar paradigm change in the way application codes are designed. EoCoE will assist the energy transition via targeted support to four renewable energy pillars: Meteo, Materials, Water and Fusion, each with a heavy reliance on numerical modelling. These four pillars will be anchored within a strong transversal multidisciplinary basis providing high-end expertise in applied mathematics and HPC. EoCoE is structured around a central Franco-German hub coordinating a pan-European network, gathering a total of 8 countries and 23 teams. Its partners are strongly engaged in both the HPC and energy fields; a prerequisite for the long-term sustainability of EoCoE and also ensuring that it is deeply integrated in the overall European strategy for HPC. The primary goal of EoCoE is to create a new, long lasting and sustainable community around computational energy science. At the same time, EoCoE is committed to deliver high-impact results within the first three years. It will resolve current bottlenecks in application codes, leading to new modelling capabilities and scientific advances among the four user communities; it will develop cutting-edge mathematical and numerical methods, and tools to foster the usage of Exascale computing. Dedicated services for laboratories and industries will be established to leverage this expertise and to foster an ecosystem around HPC for energy. EoCoE will give birth to new collaborations and working methods and will encourage widely spread best practices.

9.2.2. Collaborations with Major European Organisations

9.2.2.1. CNRS PICS NHML (2017-2019)

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

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. Informal International Partners

Four collaborations with foreign colleagues are 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. ANGE applied in 2018 to the Inria Associate Team programme in order to strenghten the collaboration.
- **USA** A joint work with R. LeVeque (Univ. Seattle) and M. Berger (New York Univ.) consists in modelling the impact of asteroids on the generation of tsunamis.
- **Germany** A collaboration with researchers from the University of Constance has been initiated in 2018 about domain decomposition and identifaction algorithms (G. Ciaramella, S. Volkwein).
- **Hong-Kong** A collaboration with F. Kwok on time parallelization for assimilation algorithm has been initiated in 2018.

9.4. International Research Visitors

- Y. Penel spent twice two weeks (May, October)at the university of Sevilla (Spain) to collaborate with E. Fernández-Nieto.

9.4.1. Visits of International Scientists

- G. Ciaramella visited J. Salomon (28.05-01.06) to work on a reduction method for identification problem.

ANTIQUE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. AnaStaSec

Title: Static Analysis for Security Properties

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2015 - December 2018

Coordinator: Inria Paris-Rocquencourt (France)

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

Inria contact: Jérôme Feret

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

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

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

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

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

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

7.1.2. REPAS

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

7.1.3. SAFTA

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

Type: ANR JCJC 2018

Duration: February 2018 - February 2022

Coordinator: Cezara Drăgoi, CR Inria

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

7.1.4. TGFSYSBIO

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

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: Plan Cancer 2014-2019

Duration: December 2015 - November 2018

Coordinator: INSERM U1085-IRSET

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

Inria contact: Jérôme Feret

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

Our project proposes a systemic approach aiming at to identifying the potential targets that regulate the shift from anti- to pro-oncogenic effects of TGF-β. To that purpose, we will combine a rule-based model (Kappa language) to describe extracellular TGF-beta activation and large-scale state-transition based (Cadbiom formalism) model for TGF-β-dependent intracellular signaling pathways. The multi-scale integrated model will be enriched with a large-scale analysis of liver tissues using shotgun proteomics to characterize protein networks from tumor microenvironment whose remodeling is responsible for extracellular activation of TGF-β. The trajectories and upstream regulators of the final model will be analyzed with symbolic model checking techniques and abstract

interpretation combined with causality analysis. Candidates will be classified with semantic-based approaches and symbolic bi-clustering technics. All efforts must ultimately converge to experimental validations of hypotheses and we will use our hepatic cellular models (HCC cell lines and hepatic stellate cells) to screen inhibitors on the behaviors of TGF-β signal.

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

7.1.5. VeriAMOS

Title: Verification of Abstract Machines for Operating Systems

Type: ANR générique 2018

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2019 - December 2022

Coordinator: Inria Paris (France)

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

Inria contact: Xavier Rival

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

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Type: IDEAS

Defi:

Instrument: ERC Proof of Concept Grant 2018

Objectif: Static Analysis for the VErification of Spreadsheets

Duration: January 2019 - June 2020

Coordinator: Inria (France)

Partner: None

Inria contact: Xavier Rival

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

7.3. International Research Visitors

7.3.1. Visits of International Scientists

7.3.1.1. Internships

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

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

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

AOSTE2 Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. FUI

9.1.1.1. CEOS

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

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

9.1.1.2. WARUNA

Participants: Liliana Cucu, Adriana Gogonel, Yves Sorel, Walid Talaboulma.

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

9.1.2. PIA

9.1.2.1. ES3CAP

Participants: Keryan Didier, Dumitru Potop Butucaru.

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

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

9.1.2.2. DEPARTS

Participants: Liliana Cucu, Adriana Gogonel, Walid Talaboulma.

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

9.2. European Initiatives

9.2.1. Collaborations in European Programs, Except FP7 & H2020

9.2.1.1. ASSUME

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

Program: ITEA

Project acronym: ASSUME

Project title: Affordable Safe and Secure Mobility Evolution

Duration: September 2015 - August 2018

Coordinator: Daimler

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

Abstract: Future mobility solutions will increasingly rely on smart components that continuously monitor the environment and assume more and more responsibility for a convenient, safe and reliable operation. Currently the single most important roadblock for this market is the ability to come up with an affordable, safe multi-core development methodology that allows industry to deliver trustworthy new functions at competitive prices. ASSUME will provide a seamless engineering methodology, which addresses this roadblock on the constructive and analytic side.

9.2.2. Collaborations with Major European Organizations

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

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

ARAMIS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. 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.

9.1.1.2. 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.

9.1.1.3. 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.

9.1.1.4. 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.

9.1.2. Inria Project Labs

9.1.2.1. 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.

9.1.3. IHU

9.1.3.1. 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.

9.1.3.2. 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.

9.1.3.3. ICM-Internal Research projects

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

Project title: Non-invasive manipulation of brain synchrony to enhance brain function and rehabilitate faulty cognition in humans: A proof of concept

Started in 2014

Coordinator: Antoni Valero Cabre (ICM-team “Dynamiques Cérébrales, Plasticité et Rééducation”)

Other partners: Service des Urgences Cérébro-Vasculaires de l’Hôpital Pitié-Salpêtrière, Paris.

The long-term goal of this project is to develop the use of non-invasive manipulation of abnormal cerebral oscillations underlying cognitive activity to restore brain function in neurological patients. Cognitive functions emerge from large distributed networks organized in space and time. The short-term goal of this application is to study the causal role played by oscillatory activity in visual awareness and test whether their manipulation by non-invasive brain stimulation has the potential to restore its function in stroke patients.

9.1.3.4. 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.

9.1.3.5. 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.

9.1.3.6. 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.

9.1.3.7. 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.

9.1.4. 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

9.1.5. Other National Programs

9.1.5.1. Programme Hospitalier de Recherche Clinique (PHRC)

Participants: Olivier Colliot, Stanley Durrleman, Didier Dormont.

- PHRC PredictPGRN, co-funding by Alzheimer Plan, *Caractérisation multimodale prospective de la démence frontotemporale dûe à des mutations du gène PGRN à un stade symptomatique et présymptomatique*. (Coordinator : A. Brice)
- PHRC ImaBio3, co-funding by Roche (pharmaceutical industry), *Rôle des réactions cellulaires sanguines, inflammatoires et immunitaires anti-amyloïde centrales et périphériques dans la maladie d'Alzheimer débutante*. (Coordinator : M. Sarazin)
- PHRC CAPP, *Caractérisation linguistique, anatomique/métabolique et biologique des différentes formes d'aphasie primaire progressive : vers le rationnel pour des essais pharmacologiques et des rééducations du langage ciblées*. (Coordinator: M. Teichmann)

9.1.5.2. Institut Universitaire d'Ingénierie pour la Santé (IUIS)

Participants: Mario Chavez, Xavier Navarro.

Project acronym: DYSPEV

Project title: Dépistage de la dyspnée par potentiels évoqués visuels

Funded in 2014

Amount: 38K€

Coordinator: Thomas Similowski

Other partners: UPMC, Inserm UMR 1158

Abstract: Steady state visual evoked potentials (SSVEP) have been widely utilized in brain computer interfacing (BCI) in last years. In this project, we explore the possibilities of SSVEP to manage the communication between patients suffering from respiratory disorders and health care providers. By imposing different breathing constraints, we use a SSVEP-based brain computer interface to help those subjects to communicate their breathing sensations (breathing well/breathing bad).

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. 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.

9.2.1.3. 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

- F. De Vico Fallani has a collaboration with the University Penn, Philadelphia, US (Prof. Danielle Bassett).
- F. De Vico Fallani has a collaboration with the University of Rome, Italy (Prof. Stefania Colonnese).
- 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).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Dr. Sarah-Christine Villeneuve spent a year from the 4th of December 2017 to the 30th of November 2018 as a clinical research fellow in Pitié Salpêtrière Hospital under the supervision of Stéphane Epelbaum (Sabbatical program).

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 runs until 2019. 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. H2020 Projects

Program: ERC Proof of Concept

Project acronym: ARTIV1

Project title: An artificial visual cortex for image processing

Duration: From April 2017 to September 2018.

Coordinator: Ugo Boscain

Abstract: The ERC starting grant GECOMETHODS, on which this POC is based, tackled problems of diffusion equations via geometric control methods. One of the most striking achievements of the project has been the development of an algorithm of image reconstruction based mainly on non-isotropic diffusion. This algorithm is bio-mimetic in the sense that it replicates the way in which the primary visual cortex V1 of mammals processes the signals arriving from the eyes. It has performances that are at the state of the art in image processing. These results together with others obtained in the ERC project show that image processing algorithms based on the functional architecture of V1 can go very far. However, the exceptional performances of the primary visual cortex V1 rely not only on the particular algorithm used, but also on the fact that such algorithm 'runs' on a dedicated hardware having the following features: 1. an exceptional level of parallelism; 2. connections that are well adapted to transmit information in a non-isotropic way as it is required by the algorithms of image reconstruction and recognition. The idea of this POC is to create a dedicated hardware (called ARTIV1) emulating the functional architecture of V1 and hence having on one hand a huge degree of parallelism and on the other hand connections among the CPUs that reflect the non-isotropic structure of the visual cortex V1.

8.3. International Research Visitors

8.3.1. Research Stays Abroad

Jean-Michel Coron was at EPFL (Switzerland) from January to June 2018.

CASCADE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives with Industry

7.1.1. CryptoComp

Program: FUI

Duration: October 2014 – November 2018

Coordinator: CryptoExperts

Partners: CEA, CNRS, Kalray, Inria, Dictao, Université de Limoges, VIACESS, Bertin technologies, GEMALTO

Local coordinator: David Pointcheval

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

7.1.2. ANBLIC

Title: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – December 2020

Coordinator: Wallix

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

Local coordinator: David Pointcheval

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

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

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

7.1.3. RISQ

Program: GDN

Duration: February 2017 – September 2020

Coordinator: Secure-IC

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

Local coordinator: Michel Abdalla

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

7.2. National Collaborations with Academics

7.2.1. EnBiD

Title: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2019

PI: Hoeteck Wee

Partners: Université Paris 2, Université Limoges

The main objective of this project is to study techniques for efficient and expressive functional encryption schemes. Functional encryption is a novel paradigm for public-key encryption that enables both fine-grained access control and selective computation on encrypted data, as is necessary to protect big, complex data in the cloud.

7.2.2. EfTrEC

Title: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – September 2020

PI: Georg Fuchsbauer

Partners: Université Paris 2

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

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

7.2.3. ALAMBIC

Title: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners: ENS Lyon, Université Limoges

The main objectives of the proposal are the following:

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

7.3. European Initiatives

7.3.1. CryptoAction

Title: Cryptography for Secure Digital Interaction

Program: H2020 ICT COST

Duration: April 2014 – April 2018

Local coordinator: Michel Abdalla

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

7.3.2. CryptoCloud

Title: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2020

PI: David Pointcheval

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

7.3.3. SAFEcrypto

Title: Secure Architectures of Future Emerging Cryptography

Program: H2020

Duration: January 2015 – January 2019

Coordinator: The Queen's University of Belfast

Partners: Inria/ENS (France), Emc Information Systems International (Ireland), Hw Communications (United Kingdom), The Queen's University of Belfast (United Kingdom), Ruhr-Universitaet Bochum (Germany), Thales Uk (United Kingdom), Universita della Svizzera italiana (Switzerland), IBM Research Zurich (Switzerland)

Local coordinator: Michel Abdalla

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

7.3.4. ECRYPT-NET

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

Program: H2020 ITN

Duration: March 2015 – February 2019

Coordinator: KU Leuven (Belgium)

Partners: KU Leuven (Belgium), Inria/ENS (France), Ruhr-Universität Bochum (Germany), Royal Holloway, University of London (UK), University of Bristol (UK), CryptoExperts (France), NXP Semiconductors (Belgium), Technische Universiteit Eindhoven (the Netherlands)

Local coordinator: Michel Abdalla

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

7.3.5. aSCEND

Title: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2020

PI: Hoeteck Wee

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

7.3.6. FENTEC

Title: Functional Encryption Technologies

Program: H2020

Duration: January 2018 – December 2020

Coordinator: ATOS Spain SA

Scientific coordinator: Michel Abdalla

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

Local coordinator: Michel Abdalla

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

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

7.4. International Initiatives with Industry

7.4.1. CryptBloC

Title: Cryptography for the Blockchain

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

Duration: October 2017 – October 2021

PI: Georg Fuchsbauer

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

7.5. International Research Visitors

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

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 (www.intphys.com)

8.2. National Initiatives

8.2.1. ANR

- Transatlantic Platform "Digging into Data". Title: "Analysis of Children's Language Experiences Around the World. (ACLEW)"; (coordinating PI : M. Soderstrom; Leader of tools development and co-PI : E. Dupoux), (2017–2020. 5 countries; Total budget: 1.4M€)

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

8.4.1.1. Internships

Internship of Diego Andai Castilla (partnership Inria-PUC-Inria Chile)

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- E. Dupoux Visiting Researcher at Facebook AI Research, Paris (Feb-Mar 2018)
- E. Dupoux Visiting Researcher at Google & DeepMind, London (April-July 2018)

DELYS Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

7.1.1.1. ESTATE - (2016–2020)

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.

7.1.1.2. 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. STIC Amsud

Title: PaDMetBio - Parallel and Distributed Metaheuristics for Structural Bioinformatics

International Partners (Institution - Laboratory - Researcher):

Universidade Federal do Rio Grande do Sul (Brazil)- Mãrcio Dorn

Universidad Nacional de San Luis (Argentina) - Verõnica Gil-Costa

Universidad de Santiago de Chile (Chile) - Mario Inostroza-Ponta

Duration: 2017 - 2018

Start year: 2017

Structural bioinformatics deals with problems where the rules that govern the biochemical processes and relations are partially known which makes hard to design efficient computational strategies for these problems. There is a wide range of unanswered questions, which cannot be answered neither by experiments nor by classical modeling and simulation approaches. Specifically, there are several problems that still do not have a computational method that can guarantee a minimum quality of solution. Two of the main challenging problems in Structural Bioinformatics are (1) the three-dimensional (3D) protein structure prediction problem (PSP) and (2) the molecular docking problem for drug design. Predicting the folded structure of a protein only from its amino acid sequence is a challenging problem in mathematical optimization. The challenge arises due to the combinatorial explosion of plausible shapes, where a long amino acid chain ends up in one out of a vast number of 3D conformations. The problem becomes harder when we have proteins with complex topologies, in this case, their predictions may be only possible with significant increases in high-performance computing power. In the case of the molecular docking problem for drug design, we need to predict the preferred orientation of a small drug candidate against a protein molecule. With the increasing availability of molecular biological structures, smarter docking approaches have become necessary. These two problems are classified as NP-Complete or NP-Hard, so there is no current computational approach that can guarantee the best solution for them in a polynomial time. Because of the above, there is the need to build smarter approaches that can deliver good solutions to the problem. In this project, we plan to explore a collaborative work for the design and implementation of population based metaheuristics, like genetic and memetic algorithms. Metaheuristics are one of the most common and powerful techniques used in this case. The main goal of this project is to gather the expertise and current work of researchers in the areas of structural bioinformatics, metaheuristics and parallel and distributed computing, in order to build novel and high quality solutions for these hot research area.

7.3.1.2. Capes-Cofecub

Title: CHOOSING - Cooperation on Hybrid cOmputing clOuds for energy savING

French Partners: Paris XI (LRI), Regal, LIG, SUPELEC

International Partners (Institution - Laboratory - Researcher):

Universidade de São Paulo - Instituto de Matemática e Estatística - Brazil, Unicamp - Instituto de Computação - Brazil

Duration: 2014–2018

The cloud computing is an important factor for environmentally sustainable development. If, in the one hand, the increasing demand of users drive the creation of large datacenters, in the other hand, cloud computing's "multitenancy" trait allows the reduction of physical hardware and, therefore, the saving of energy. Thus, it is imperative to optimize the energy consumption corresponding to the datacenter's activities. Three elements are crucial on energy consumption of a cloud platform: computation (processing), storage and network infrastructure. Therefore, the aim of this project is to provide different techniques to reduce energy consumption regarding these three elements. Our work mainly focuses on energy saving aspects based on virtualization, i.e., pursuing the idea of the intensive migration of classical storage/processing systems to virtual ones. We will study how different organizations (whose resources are combined as hybrid clouds) can cooperate with each other in order to minimize the energy consumption without the detriment of client requirements or quality of service. Then, we intend to propose efficient algorithmic solutions and design new coordination mechanisms that incentive cloud providers to collaborate.

7.3.1.3. 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.

DYOGENE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. 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. S. Meyn [Unversity of Florida] was invited professor by LINCS and ENS from July to December 2018.

8.1.2. PGMO

Dyogene participates to 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). Post-doc Cheng Wan was financed by this project from Feb-Nov 2018.

8.2. National Initiatives

8.2.1. 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. This year DYOGENE has co-organized yearly conference of the GdR *Stochastic Geometry Days 2018* 14–18 mai 2018 Paris (France); https://geosto-2018.sciencesconf.org/.

8.2.2. 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

8.2.3. 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.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. 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. B. Błaszczyszyn was visiting ISI Bangalore for two weeks in November–December 2018.

8.3.1.2. 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).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- D. Yogeshwaran [Indian Statistical Institute, Bangalore, India]
- S. Meyn [University of Florida, USA] was invited Prof at ENS and LINCS, July - December 2018

8.4.1.1. Internships

- Master Probabilités et Modèles aléatoires UPMC, Walid Ghanem, *Hydrodynamic limit of a network with moving servers*, 04-07/2018, encadrant Christine Fricker.
- Master MASH (Mathématiques appliquées aux sciences humaines) ENS-Paris Dauphine University, *Using customer oriented policies based on probabilistic methods to enhance the Bike Sharing System Velib'*, 08-011/2018, encadrants Christine Fricker et Laurent Massoulié.
- Akshay Goel [Kyushu University, Fukuoka, Japan] Mars 2018,
- Tokuyama Kiichi [Tokyo Tech, Tokyo, Japan], April 2018,

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

- B. Błaszczyszyn was visiting Yogeshwaran D. at the Indian Statistical Institute Bangalore for two weeks in November–December 2018 (IFCAM project).
- A. Busic was a long-term participant (March-Mai 2018) of the Real-Time Decision Making program, Simons Institute, UC Berkeley, USA; https://simons.berkeley.edu/programs/realtime2018

EVA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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.

9.1.2. 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 exploits the Cap d'Agde marina, as part of the SmartMarina project.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

The H2020 following projects are ongoing:

- H2020 SPARTA, Jan 2019 – December 2020.
- H2020 F-Interop, http://f-interop.eu/, Nov 2015 – Oct 2018.
- H2020 ARMOUR, https://www.armour-project.eu/, Feb 2016 – Jan 2018.

9.2.2. Collaborations with Major European Organizations

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. 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.

9.3.1.2. DIVERSITY

- Title: Measuring and Exploiting Diversity in Low-Power Wireless Networks
- International Partner (Institution - Laboratory - Researcher):
  - University of Southern California (United States) - Autonomous Networks Research Group (ANRG) - Bhaskar Krishnamachari
- Start year: 2016
- The goal of the DIVERSITY associate team is to develop the networking technology for tomorrow's Smart Factory. The two teams comes with a perfectly complementary background on standardization and experimentation (Inria-EVA) and scheduling techniques (USC-ANRG). The key topic addressed by the joint team will be networking solutions for the Industrial Internet of Things (IIoT), with a particular focus on reliability and determinism.

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-lead 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 part.

9.3.2.2. Informal International Partners

The Inria-EVA 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.

9.3.2.3. International Initiatives

Inria-EVA participates in the IoT Benchmarks Initiative (https://www.iotbench.ethz.ch/)

Inria-EVA will be participating in 2019 in the WirelessWine SticAm-Sud project.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

1. **Prof. Xavi Vilajosana (UOC/OpenMote)** (26-30 November 2018) working on OpenMote B bring-up with Tengfei Chang and **Thomas Watteyne**
2. **Brian Gregory Kilberg (UC Berkeley)** (11-18 September 2018) working on OpenWSN/ROS integration with **Thomas Watteyne** and Tengfei Chang
3. **Prof. Xavi Vilajosana (UOC/OpenMote)** (24-28 June 2018) working on F-Interop 6TiSCH with **Thomas Watteyne** and Tengfei Chang
4. **Pablo Modernell (UOC)** (28 May – 1 June 2018) working on F-Interop with Tengfei Chang and **Thomas Watteyne**
5. **Malisa Vucinic (U Montenegro)** (9 -16 March 2018) working on 6TiSCH Security with **Thomas Watteyne**
6. **Lance Doherty (Analog Devices)** (8-9 February 2018) working on SmartMesh IP with **Thomas Watteyne**
7. **Malisa Vucinic (U Montenegro)** (29 January-16 February 2018) working on 6TiSCH Security with **Thomas Watteyne**

9.4.2. Internships

1. **Felipe Moran**, MSc intern from ENSTA ParisTech (1 September 2017 – 31 August 2018), EDF fellow, Research Topic: mote feeding habits, SmartMesh IP, Advisor: Thomas Watteyne
2. **Fabian Rincon Vija**, MSc intern from ENSTA ParisTech (14 May – 31 August 2018), Research Topic: Extension of F-Interop to IEEE 802.15.4 sub-GHz, Advisor: Thomas Watteyne
3. **Marcelo Augusto Ferreira**, MSc intern from ENSTA ParisTech (1 May – 31 August 2018), Research Topic: Measuring Energy Consumption in F-Interop, Advisor: Thomas Watteyne
4. **Imene Ben Haddada**, Using Support Vector Machine for Positioning Services in Vehicle Ad-hoc NETworks (ENSI- Tunisia), March-July 2018.
5. **Khalifa Hadded**, Generation of positioning data in Vehicle Ad-hoc NETworks (ENSI- Tunisia), March-July 2018.
6. **Zied Soua**, Formation d'un réseau TSCH
   et ordonnancement de ses communications dans le cadre de l'IoT industriel, (INSAT- Tunisia), February-July 2018.

9.4.3. Visits to International Teams

9.4.3.1. Research Stays Abroad

- **Thomas Watteyne** spent the month of August 2017 at UC Berkeley, working with Prof. Glaser on the SnowHow project, and with Prof. Pister on Smart Dust and OpenWSN.
- Tengfei Chang spent the month of July 2017 in California working with Prof. Pister working on Smart Dust UC Berkeley, and Prof. Krishnamachari working on testbed deployment at the Univesity of Southern California.

GALLIUM Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR projects

9.1.1.1. Vocal

Participants: Armaël Guéneau, Xavier Leroy, François Pottier.

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

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

9.1.2. FUI Projects

9.1.2.1. Secur-OCaml

Participants: Damien Doligez, Fabrice Le Fessant.

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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. Deepsea

Participants: Umut Acar, Vitaly Aksenov, Arthur Charguéraud, Adrien Guatto, Michael Rainey.

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

9.2.2. ITEA3 Projects

9.2.2.1. Assume

Participants: Gergö Barany, Xavier Leroy, Luc Maranget.

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

9.3. International Initiatives

9.3.1. Informal International Partners

- Princeton University: interactions between the CompCert verified C compiler and the Verified Software Toolchain developed at Princeton.
- The University of Cambridge and ARM Ltd, Cambridge and Imperial College London: formal modeling and testing of weak memory models.

GANG Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

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

Gang is participating to the LINCS, a research centre co-founded by Inria, Institut Mines-Télécom, UPMC and Alcatel-Lucent Bell Labs, dedicated to research and innovation in the domains of future information and communication networks, systems and services. Gang contributes to work on online social networks, content centric networking and forwarding information verification.

9.2. National Initiatives

9.2.1. ANR DESCARTES

Participants: Carole Delporte-Gallet, 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.

9.2.2. 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.

9.2.3. ANR FREDDA

Participants: Carole Delporte-Gallet, 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.

9.2.4. 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.

9.2.5. 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.

9.3. European Initiatives

9.3.1. 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.

9.3.2. 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.

9.4. International Initiatives

9.4.1. 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/).

9.4.2. Inria International Partners

9.4.2.1. 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).

Lalla Moutadib, PhD student at Uinversity of Toronto, directed by Alan Borodin and Derek Corneil but also unformally by Michel Habib. 2 visits in 2018 in our group. She got her PhD in september 2018. See https://tspace.library.utoronto.ca/handle/1807/92081.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- Sergio Rajsbaum (UNAM Mexico) - April 1 to June 30.
- Giuliano Losa (UCLA USA)- May 17 to May 30.

9.5.2. Visits to International Teams

- Carole Delporte and Hugues Fauconnier have visited Sergio Rajsbaum at UNAM Mexico - September 2 to September 14.

MAMBA Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. 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.

9.1.1.2. 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 REO team, Inria Paris. The pursued objective is the bioengineering design of an artificial liver intended for liver replacement.

9.1.1.3. ANR InTelo 2017-2020

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

9.1.1.4. 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).

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

9.1.2.1. ITMO Cancer EcoAML

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

9.1.2.2. ITMO Cancer MoGlImaging

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

9.2. European Initiatives

9.2.1. Collaborations in European Programs, Except FP7 & H2020

Program: Celtic+

Project acronym: Sendate

Project title:Secure Networking for a Data Center Cloud in Europe

April 2016/May 2019

Coordinator: Nokia

Other partners: Siemens, IMT, ...

9.3. International Initiatives

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

9.3.1.1. 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 are presently maintained and ensured by the sabbatical of Marie Doumic – MAMBA team leader –, 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).

Of note, C. Schmeiser has been a laureate for the "Chaire d'excellence" program of the FSMP. As such, he is for six months in Paris, and delivered a course at IHP on entropy methods. Many of his students and collaborators visited him (D. Oelz, G. Jankowiak, L. Kanzler, G. Favre, L. Neumann...), and participated to a joint Mamba-MaMoCeMa meeting on December 6th, still strengthening our links.

9.3.2. Participation in Other International Programs

9.3.2.1. International Initiatives

ECOS Nord C17M01

Title: News methods for controle of dengue and arobivroses epidemics

International Partner (Institution - Laboratory - Researcher):

Universidad del Valle (Colombia) - Department of Mathematics - Olga Vasilieva

Duration: 2017 - 2019

Start year: 2017

The overall goal of the project is the development of mathematical models and theory-based control methods, contributing to the improvement of epidemiological surveillance and the control of dengue and other serious diseases transmitted by mosquitoes Aedes aegypti (chikungunya, yellow fever, zika fever). More specifically, it :

- Develops modeling framework for the biological control of mosquito populations (through the use of natural predators, Wolbachia bacteria etc.).
- Proposes and evaluates control strategies based on the use of biological agents and on their possible combinations with traditional control measures (such as removal of reproduction, spraying insecticides and / or larvicides, use of mosquito nets, repellents, etc.).
- Compares the results of biological control strategies (and their combinations) with those of traditional control using a cost / efficiency approach.
- Includes in the developments the spatial aspects of the questions above.

BMBF (Germany) / LiSym; 2016-2020 LiSym addresses liver diseases and regeneration, namely, steatosis, fibrosis and cirrhosis, and acute on chronic liver failure. Dirk Drasdo is co-coordinator of one sub-project, participant in one of the other ones, and member of the leadership board

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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Prof. Olga Vasilieva (Universidade del Valle, Cali, Colombia) was invited during three weeks, together with Edwin Bairros, PhD student.
- Prof. Yukihiko Nakata (Shimane University, Matsue, Japan) was hosted during one week in the framework of the French program Exploration France.
- Prof. C. Schmeiser (university of Vienna, Austria) was visiting during four month, from september 2018, and should stay until february 2019.
- Prof. D. Oelz (university of Queensland, Australia) visited from Dec. 5th to Dec. 21st.
- Jieling Zhao, Postdoc from IfADo
- Paul van Liedekerke, Research engineer from IfADo

9.4.1.1. Internships

Ismael Gonzalez Valverde (University of Zaragoza) visited our team for 3 months working on implementation of the meshing of liver micro-structures in modeling of liver regeneration within TiSim.

9.4.2. Visits to International Teams

9.4.2.1. Sabbatical programme

Marie Doumic was in Vienna for a sabbatical stay until July 2018.

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 (2016-2020) to investigate new numerical models of solid transport in rivers.
- 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 (2015-2019), PI: Y. Maday, Sorbonne Université. This project is concerned with parallel-in-time algorithms.
- 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)
- REST (theoretical spectroscopy),
- CHOCOLAS (experimental and numerical study of shock waves).

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

8.2. European Initiatives

The ERC consolidator Grant MSMATH (ERC Grant Agreement number 614492, PI T. Lelièvre) is running (it started in June 2014).

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, Inria 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. Informal International Partners

- Center of Excellence program in Mathematics and Life Sciences at the Department of Mathematics, University of Oslo, Norway, (B. Øksendal).
- Kings College, London (R. Dumitrescu)
- Department of Mathematics, University of Manchester (Tusheng Zhang, currently in charge of an EU-ITN program on BSDEs and Applications).
- Kensas University (Yaozhong Hu)
- Cornell University, ORIE department (Andreea Minca)
- Mannheim University (Alexander Schied, Chair of Mathematics in Business and Economics, Department of Mathematics)
- 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)

9.3.2. Internships

Oussama Bellalah, Inria, May-August

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 CityLab@Inria

Participants: Valérie Issarny, Bruno Lefèvre.

- **Name:** CityLab@Inria – *Overcoming the Smart City Challenge – Toward Environmental and Social Sustainability*
- **Period:** [January 2014 – November 2018]
- **Inria teams:** CLIME/ANGE, DICE, FUN, MIMOVE, MYRIADS, SMIS/PETRUS, URBANET/AGORA
- **URL:** http://citylab.inria.fr

The Inria Project Lab (IPL) CityLab@Inria studies ICT solutions toward smart cities that promote both social and environmental sustainability. A strong emphasis of the Lab is on the undertaking of a multi-disciplinary research program through the integration of relevant scientific and technology studies, from sensing up to analytics and advanced applications, so as to actually enact the foreseen smart city Systems of Systems. Obviously, running experiments is a central concern of the Lab, so that we are able to confront proposed approaches to actual settings.

9.1.1.2. Inria IPL BetterNet

Participants: Renata Teixeira, Vassilis Christophides, Francesco Bronzino.

- **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.

9.1.1.3. Inria ADT MOSQUITO

Participants: Renata Teixeira, Francesco Bronzino.

- **Name:** MOSQUITO – *A mobile platform to measure the quality of Internet connectivity*
- **Period:** [November 2016 – October 2018]
- **Partners:** Inria MiMove, Inria SPIRALS.

The ADT MOSQUITO is part of the Inria Project Lab (IPL) initiative BetterNet. This ADT project focuses on the design and the development of a measurement platform for the quality of mobile Internet access by federating the existing mobile platforms identified in the BetterNet IPL. Beyond the priceless value of such a measurement platform for the research community, this ADT also aims to publish live reports on the quality of mobile Internet access through the BetterNet initiative.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. H2020 ICT FIESTA-IoT

Participants: Valérie Issarny, Nikolaos Georgantas, Rachit Agarwal.

Name: FIESTA-IoT – *Federated Interoperable Semantic IoT/cloud Testbeds and Applications*

URL: http://fiesta-iot.eu

Type: Research & Innovation Action (ICT)

Topic: FIRE+ (Future Internet Research & Experimentation)

Period: [February 2015 - January 2018]

Partners: Fraunhofer FOKUS (Germany) [**coordinator**], INSIGHT @ National University of Galway (Ireland) [**co-coordinator**], University of Southampton IT Innovation Centre (UK), Inria MiMove, University of Surrey (UK), Unparallel Innovation Lda (Portugal), Easy Global Market (France), NEC Europe Ltd (UK), University of Cantabria (Spain), Com4innov (France), Athens Information Technology (Greece), SOCIEDAD PARA EL DESARROLLO REGIONAL DE CANTABRIA (Spain), Ayuntamiento de Santander (Spain), Korea Electronics Technology Institute (Korea).

Despite the proliferation of IoT and smart cities testbeds, there is still no easy way to conduct large scale experiments that leverage data and resources from multiple geographically and administratively distributed IoT platforms. Recent advances in IoT semantic interoperability provide a sound basis for implementing novel cloud-based infrastructures that could allow testbed-agnostic access to IoT data and resources. FIESTA will open new horizons in IoT experimentation at a global scale, based on the interconnection and interoperability of diverse IoT testbeds. FIESTA will produce a first-of-a-kind blueprint experimental infrastructure (tools, techniques and best practices) enabling testbed operators to interconnect their facilities in an interoperable way, while at the same time facilitating researchers in deploying integrated experiments, which seamlessly transcend the boundaries of multiple IoT platforms. FIESTA will be validated and evaluated based on the interconnection of four testbeds (in Spain, UK, France and Korea), as well as based on the execution of novel experiments in the areas of mobile crowd-sensing, IoT applications portability, and dynamic intelligent discovery of IoT resources. In order to achieve global outreach and maximum impact, FIESTA will integrate an additional testbed and experiments from Korea, while it will also collaborate with IoT experts from USA. The participation of a Korean partner (based its own funding) will maximize FIESTA's value for EC money. Moreover, the project will take advantage of open calls processes towards attracting third-parties that will engage in the integration of their platforms within FIESTA or in the conduction of added-value experiments. As part of its sustainability strategy, FIESTA will establish a global market confidence programme for IoT interoperability, which will enable innovative platform providers and solution integrators to ensure/certify the openness and interoperability of their developments.

9.3. International Initiatives

9.3.1. Inria International Labs

Inria@SiliconValley

Associate Team involved in the International Lab:

9.3.1.1. MINES

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

International Partner:

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.

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

9.3.2.1. HOMENET

Title: Home network diagnosis and security

International Partner:

Princeton University (United States) - Computer Science Department - 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 MiMove brings an existing Web-based measurement platform, and expertise in traffic-based profiling and anomaly detection.

9.3.2.2. ACHOR

Title: Adaptive enactment of service choreographies

International Partner:

Universidade Federal de Goiás (Brazil) - Computer Science Department - Fabio Costa

Start year: 2016

See also: http://www.inf.ufg.br/projects/achor

Service choreographies are distributed compositions of services (e.g., Web services) that coordinate their execution and interactions without centralized control. Due to this decentralized coordination and the ability to compose third-party services, choreographies have shown great potential as an approach to automate the construction of large-scale, on-demand, distributed applications. Technologies to enable this approach are reaching maturity level, such as modeling languages for choreography specification and engines that operate the deployment of services and enactment of choreographies at Future Internet scales. Nevertheless, a number of problems remain open on the way to fully realize the approach, among them: (i) Deployment of multiple choreographies on top of a collection of shared services (considering service sharing as an effective way to increase the utilization of resources); (ii) Dynamic adaptation of functional and non-functional properties due to runtime changes in the environment and user requirements (adapting the set of services and/or the resources used to run the services in order to add/remove/change functions and maintain QoS properties, respectively); and (iii) Seamless and dynamic integration of mobile services (e.g., smartphone apps, sensors and actuators on handhelds and wearables) and cloud- based services (including the need to consider: mobility of both devices and services, resource constraints of mobile devices, temporary disconnection, interoperability between different interaction paradigms (message-passing, event-based, data-sharing) at the middleware layer, and effect of these paradigms on end-to-end QoS). The overall goal of the project is to design an architecture for adaptive middleware to support service choreographies in large-scale scenarios that involve dynamicity and diversity in terms of application requirements, service interaction protocols, and the use of shared local, mobile and cloud resources.

9.3.3. Inria International Partners

9.3.3.1. Informal International Partners

- Northeastern University (Prof. David Choffnes): We are working on methods based on active probing to diagnose poor video quality.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Mark Crovella from Boston University is visiting professor at Inria.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

- Valérie Issarny was visiting scholar at the EECS Department at UC Berkeley till August 2018. She was hosted by CITRIS in the context of which she was carrying out collaborative research in the area of smart cities and acting as scientific coordinator of the Inria@SiliconValley program.
- Renata Teixeira is visiting scholar at the Computer Science department at Stanford University.
- Georgios Bouloukakis is Inria postdoctoral fellow at University of California, Irvine, in the context of the Inria@SiliconValley program.

MOKAPLAN Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

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.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

J-D. Benamou and G. Rukhaia are members of the ROMSOC ITN.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Shuangjian Zhang, (PostDoc), Université de Toronto, June-August 2018.
- Clarice Poon, Imperial College London, January 2018
- Teresa Radice, Université de Naples, many short stays.

7.3.2. Visits to International Teams

7.3.2.1. Research Stays Abroad

- P. Pegon was invited for 10 days to Penn State College by Alberto Bressan in order to start a collaboration on the theory of ramified transport and applications to biology, and to give lectures (2) in the seminar series on Computational and Applied Mathematics.
- G. Carlier was a John von Neumann invited Professor at TUM (Munich) in 2018.

OURAGAN Team

9. Partnerships and Cooperations

9.1. European Initiatives

9.1.1. FP7 & H2020 Projects

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

Project acronym: Almacrypt

Project title: Algorithmic and Mathematical Cryptology

Duration: 01/2016 - 12/2010

Coordinator: Antoine Joux

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

9.2. International Initiatives

9.2.1. Inria International Labs

9.2.1.1. Informal International Partners

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

9.3. International Research Visitors

9.3.1. Visits of International Scientists

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

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

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

8.1.1. ANR

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

8.1.2. FUI: Fonds unique interministériel

Modeliscale contract (AAP-24). Using Modelica at scale to model and simulate very large Cyber-Physical Systems. Principal industrial partner: Dassault-Systèmes. Inria contacts are Benoit Caillaud (HYCOMES, Rennes) and Marc Pouzet (PARKAS, Paris).

8.1.3. Others

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

8.2. European Initiatives

8.2.1. H2020 Projects

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

Project acronym: TETRAMAX

Project title: Technology Transfer via Multinational Application Experiments

Duration: September 2017 – August 2021

Coordinator: Rainer Leupers

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

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

8.2.2. Collaborations in European Programs, Except FP7 & H2020

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

8.3. International Initiatives

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

8.3.1.1. POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages
International Partner (Institution - Laboratory - Researcher):

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

Start year: 2016
See also: http://polyflow.gforge.inria.fr
The objective of the associate team is to foster collaborations on fundamental and applied research. It also supports training sessions, exchange of undergraduate and master students, and highlighting opportunities in the partners' research, education and economic environments.

Polyhedral techniques for program transformation are now used in several proprietary and open source compilers. However, most of the research on polyhedral compilation has focused on imperative languages, where computation is specified in terms of computational statements within nested loops and control structures. Graphical data-flow languages, where there is no notion of statements or a schedule specifying their relative execution order, have so far not been studied using a powerful transformation or optimization approach. These languages are extremely popular in the system analysis, modeling and design of embedded reactive control applications. They also underline the construction of domain-specific languages and compiler intermediate representations. The execution semantics of data-flow languages impose a different set of challenges for compilation and optimization. We are studying techniques enabling the extraction of a polyhedral representation from data-flow programs, to transform them with the goal of generating memory-efficient and high-performance code for modern architectures.

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

8.3.2. Participation in Other International Programs

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

8.3.2.1. Indo-French Center of Applied Mathematics

POLYFLOW

Title: Polyhedral Compilation for Data-Flow Programming Languages

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (India) - Uday Kumar Reddy Bondhugula

Duration: 2016 - 2018

Start year: 2016

The objective of the associate team is to foster collaborations on fundamental and applied research. It also supports training sessions, exchange of undergraduate and master students, and highlighting opportunities in the partners' research, education and economic environments. Polyhedral techniques for program transformation are now used in several proprietary and open source compilers. However, most of the research on polyhedral compilation has focused on imperative languages, where computation is specified in terms of computational statements within nested loops and control structures. Graphical data-flow languages, where there is no notion of statements or a schedule specifying their relative execution order, have so far not been studied using a powerful transformation or optimization approach. These languages are extremely popular in the system analysis, modeling and design of embedded reactive control applications. They also underline the construction of domain-specific languages and compiler intermediate representations. The execution semantics of data-flow languages impose a different set of challenges for compilation and optimization. We are studying techniques enabling the extraction of a polyhedral representation from data-flow programs, to transform them with the goal of generating memory-efficient and high-performance code for modern architectures. The research conducted in PolyFlow covers both fundamental and applied aspects. The partners also emphasize the development of solid research tools. The associate team will facilitate their dissemination as free software and their exploitation through industrial collaborations.

PI.R2 Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

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

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

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

Yann Régis-Gianas collaborates with Mitsubishi Rennes on the topic of differential semantics. This collaboration led to the CIFRE grant for the PhD of Thibaut Girka.

Yann Régis-Gianas collaborates with ANSSI on the topic of certified ful programming in Coq.

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

Yann Régis-Gianas and Alexis Saurin (coordinator) are members of the four-year RAPIDO ANR project, started in January 2015. RAPIDO aims at investigating the use of proof-theoretical methods to reason and program on infinite data objects. The goal of the project is to develop logical systems capturing infinite proofs (proof systems with least and greatest fixpoints as well as infinitary proof systems), to design and to study programming languages for manipulating infinite data such as streams both from a syntactical and semantical point of view. Moreover, the ambition of the project is to apply the fundamental results obtained from the proof-theoretical investigations (i) to the development of software tools dedicated to the reasoning about programs computing on infinite data, *e.g.* stream programs (more generally coinductive programs), and (ii) to the study of properties of automata on infinite words and trees from a proof-theoretical perspective with an eye towards model-checking problems. Other permanent members of the project are Christine Tasson from IRIF (PPS team), David Baelde from LSV, ENS-Cachan, and Pierre Clairambault, Damien Pous and Colin Riba from LIP, ENS-Lyon.

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

7.2. European Initiatives

7.2.1. Collaborations in European Programs, Except FP7 & H2020

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

Presentation of EUTYPES: Types are pervasive in programming and information technology. A type defines a formal interface between software components, allowing the automatic verification of their connections, and greatly enhancing the robustness and reliability of computations and communications. In rich dependent type theories, the full functional specification of a program can be expressed as a type. Type systems have rapidly evolved over the past years, becoming more sophisticated, capturing new aspects of the behaviour of programs and the dynamics of their execution. This COST Action will give a strong impetus to research on type theory and its many applications in computer science, by promoting (1) the synergy between theoretical computer scientists, logicians and mathematicians to develop new foundations for type theory, for example as based on the recent development of "homotopy type theory", (2) the joint development of type theoretic tools as proof assistants and integrated programming environments, (3) the study of dependent types for programming and its deployment in software development, (4) the study of dependent types for verification and its deployment in software analysis and verification. The action will also tie together these different areas and promote cross-fertilisation.

7.3. International Initiatives

7.3.1. IIL projects

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

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

7.3.2.1. Associate team

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

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

7.3.2.2. Joint Inria-CAS project

Pierre-Louis Curien is principal investigator on the French side for a joint project Inria - Chinese Academy of Sciences. The project's title is "Verification, Interaction, and Proofs". The principal investigator on the Chinese side is Ying Jiang, from the Institute of Software (ISCAS) in Beijing. The participants of the project on the French side are Pierre-Louis Curien and Jean-Jacques Lévy, as well as other members of IRIF (Thomas Ehrhard, Jean Krivine, Giovanni Bernardi, Ahmed Bouajjani, Mihaela Sighireanu, Constantin Enea, Gustavo Petri), and Gilles Dowek (Deducteam team of Inria Saclay). On the Chinese side, the participants are Ying Jiang, as well as other members of the ISCAS (Angsheng Li, Xinxin Liu, Yi Lü, Peng Wu, Yan Rongjie, Zhilin Wu, and Wenhui Zhang), and Yuxi Fu (from Shanghai Jiaotong University). The project funds the postdoc of Kailiang Ji at University Paris 7, that started in December 2017 and will end in Marche 2019.

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

7.3.3. Inria International Partners

7.3.3.1. Informal International Partners

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

7.4. International Research Visitors

7.4.1. Visits of International Scientists

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

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

7.4.2. Internships

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

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

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

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

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

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

7.4.3. Research Stays Abroad

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

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

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

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **French Ministry of Armies**

  POLSYS has a collaboration with the French Ministry of Armies.

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

  GLOBAL ALGEBRAIC SHOOTING METHOD IN OPTIMAL CONTROL AND APPLICATIONS

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

8.2. National Initiatives

8.2.1. ANR

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

  `Duration:` 2018–2022

  GALOP [0] is a Young Researchers (JCJC) project with the purpose of extending the limits of the state-of-the-art algebraic tools in computer science, especially in stochastic games. It brings original and innovative algebraic tools, based on symbolic-numeric computing, that exploit the geometry and the structure and complement the state-of-the-art. We support our theoretical tools with a highly efficient open-source software for solving polynomials. Using our algebraic tools we study the geometry of the central curve of (semi-definite) optimization problems. The algebraic tools and our results from the geometry of optimization pave the way to introduce algorithms and precise bounds for stochastic games.

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

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

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

  The RISQ [0] project is certainly the biggest industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the call Grands DΓ©fis du NumΓ©rique which is managed by BPI France, and will be funded thanks to the so-called Plan d'Investissements d'Avenir.

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

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

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

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

  Duration: 2018–2022

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

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

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

  Duration: 2019-2022.

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

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

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

8.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: CryptoAction

Project title: Cryptography for Secure Digital Interaction

Duration: Apr. 2014 - Apr. 2018

Coordinator: Claudio ORLANDI

Abstract: As increasing amounts of sensitive data are exchanged and processed every day on the Internet, the need for security is paramount. Cryptography is the fundamental tool for securing digital interactions, and allows much more than secure communication: recent breakthroughs in cryptography enable the protection - at least from a theoretical point of view - of any interactive data processing task. This includes electronic voting, outsourcing of storage and computation, e-payments, electronic auctions, etc. However, as cryptography advances and becomes more complex, single research groups become specialized and lose contact with "the big picture". Fragmentation in this field can be dangerous, as a chain is only as strong as its weakest link. To ensure that the ideas produced in Europe's many excellent research groups will have a practical impact, coordination among national efforts and different skills is needed. The aim of this COST Action is to stimulate interaction between the different national efforts in order to develop new cryptographic solutions and to evaluate the security of deployed algorithms with applications to the secure digital interactions between citizens, companies and governments. The Action will foster a network of European research centers thus promoting movement of ideas and people between partners.

Program: COST

Project acronym: CRYPTACUS

Project title: Cryptanalysis of ubiquitous computing systems

Duration: Dec. 2014 - Dec. 2018

Coordinator: Gildas AVOINE

Abstract: Recent technological advances in hardware and software have irrevocably affected the classical picture of computing systems. Today, these no longer consist only of connected servers, but involve a wide range of pervasive and embedded devices, leading to the concept of “ubiquitous computing systems”. The objective of the Action is to improve and adapt the existent cryptanalysis methodologies and tools to the ubiquitous computing framework. Cryptanalysis, which is the assessment of theoretical and practical cryptographic mechanisms designed to ensure security and privacy, will be implemented along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems. Researchers have only recently started to focus on the security of ubiquitous computing systems. Despite the critical flaws found, the required highly-specialized skills and the isolation of the involved disciplines are a true barrier for identifying additional issues. The Action will establish a network of complementary skills, so that expertise in cryptography, information security, privacy, and embedded systems can be put to work together. The outcome will directly help industry stakeholders and regulatory bodies to increase security and privacy in ubiquitous computing systems, in order to eventually make citizens better protected in their everyday life.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

8.4.1.1. Internships

Reine Abi Rached

Date: Apr. 2018 - Aug. 2018

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

Supervisor: Jean-Charles Faugère, Jérémy Berthomieu

Hadrien Brochet

Date: Jun. 2018 - Aug. 2018

Institution: ENS Lyon

Supervisor: Elias Tsigaridas

Phuoc Le

Date: Apr. 2018 - Aug. 2018

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

Supervisor: Jean-Charles Faugère, Mohab Safey El Din

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

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

PROSECCO Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

8.1.1.1. AnaStaSec

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

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

Duration: January 2015 - September 2019.

Coordinator: Jérôme Féret, EPI Antique, Inria Paris (France)

Participant: Bruno Blanchet

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

8.1.1.2. AJACS

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

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

Duration: October 2014 - March 2019.

Coordinator: Alan Schmitt, Inria (France)

Participants: Karthikeyan Bhargavan, Bruno Blanchet, Nadim Kobeissi

Abstract: The goal of the AJACS project is to provide strong security and privacy guarantees for web application scripts. To this end, we propose to define a mechanized semantics of the full JavaScript language, the most widely used language for the Web, to develop and prove correct analyses for JavaScript programs, and to design and certify security and privacy enforcement mechanisms.

8.1.1.3. SafeTLS

Title: SafeTLS: La sécurisation de l'Internet du futur avec TLS 1.

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

Duration: October 2016 - September 2020

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

Participants: Karthikeyan Bhargavan

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

8.1.1.4. TECAP

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

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

Duration: January 2018 - December 20

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

Participants: Bruno Blanchet, Benjamin Lipp

Abstract: A large variety of automated verification tools have been developed to prove or find attacks on security protocols. These tools differ in their scope, degree of automation, and attacker models. The aim of this project is to get the best of all these tools, meaning, on the one hand, to improve the theory and implementations of each individual tool towards the strengths of the others and, on the other hand, build bridges that allow the cooperations of the methods/tools. We will focus in this project on the tools CryptoVerif, EasyCrypt, Scary, ProVerif, Tamarin, AKiSs and APTE.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. ERC Consolidator Grant: CIRCUS

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

Duration: April 2016 - March 2021

Coordinator: Karthikeyan Bhargavan, Inria

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

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

8.2.1.2. ERC Starting Grant: SECOMP

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

Duration: Jan 2017 - December 2021

Coordinator: Catalin Hritcu, Inria

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

8.2.1.3. NEXTLEAP

Title: NEXTLEAP: NEXT generation Legal Encryption And Privacy

Programm: H2020

Duration: January 2016 - December 2018

Coordinator: Harry Halpin, Inria

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

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

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

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

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

8.3.2. Participation in Other International Programs

8.3.2.1. SSITH/HOPE

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

Program: DARPA SSITH

Duration: December 2017 - February 2021

Coordinator: Charles Stark Draper Laboratory

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

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

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

MIT, as well as industry collaborators from DornerWorks and Dover Microsystems. In addition to Draper's in-house expertise in hardware design, cyber-security (defensive and offensive, hardware and software) and formal methods, the HOPE team includes experts from all domains relevant to SSITH, including (a) computer architecture: DeHon (Penn), Shrobe (MIT); (b) formal methods including programming languages and security: Pierce (Penn), Tolmach (PSU), Hritcu (Inria); and (c) operating system integration (DornerWorks). Dover Microsystems is a spin-out from Draper that will commercialize concepts from the Draper ISP project.

8.3.2.2. Everest Expedition

Program: Microsoft Expedition and MSR-Inria Collaborative Research Project

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

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

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

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

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

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

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

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

https://project-everest.github.io

8.4. International Research Visitors

8.4.1. Visits of International Scientists

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

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

8.4.1.1. Internships

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

8.4.2. Visits to International Teams

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

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 project Sputthy**: Zaki Leghtas has received 50k euros from the DIM SIRTEQ to purchase a sputtering system. With this machine, we will fabricate high quality resonators made out of Niobium and high kinetic inductance material such as NbTiN.
- **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.
- **FSMP postdoctoral fellowship**: Paolo Forni has been selected for a postdoctoral fellowship by the Fondation des Sciences Mathématiques de Paris (FSMP) for the academic year 2018-2019: this 12-month postdoc fellowship extends a previous one supported by the programme Math-PSL of PSL Research University.

7.2. National Initiatives

- **ANR project GEARED**: This four-year collaborative ANR project, entitled “Reservoir engineering quantum entanglement in the microwave domain” and coordinated by Mazyar Mirrahimi, started on October 2014 and ended on September 2018. The participants of the project were Mazyar Mirrahimi (QUANTIC project-team), Benjamin Huard (ENS Lyon), Daniel Esteve and Fabien Portier (Quantronics group, CEA Saclay), Nicolas Roch and Olivier Buisson (Institut Neel, Grenoble). This project deals with robust generation of entanglement as a key resource for quantum information processing (quantum simulation, computation and communication). QUANTIC receieved a funding of 114k in this framework.
- **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 will start on april 2019 and will run for 4 years.

7.3. European Initiatives

7.3.1. 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 collaborating with Samuel Deleglise and Emmanuel Flurin from Laboratoire Kastler Brossel to understand and analyze their experimental data. In this aim, we have developed new adiabatic elimination techniques for multi-partite open quantum systems with non-trivial zero-order dynamics.

Partner 3: University of Padova

Alain Sarlette has been pursuing a fruitful collaboration with the group of Francesco Ticozzi on "dynamical systems aspects of quantum systems". A novel line of work in the direction of quantum thermalization and quantum random walks has been explored, in the framework of the PhD of S. Apers (Ghent University) supervised by A. Sarlette.

Partner 4: Ghent University.

Alain Sarlette has been collaborating with applied mathematicians interested in quantum control at UGent (Dirk Aeyels, Lode Wylleman, Gert De Cooman) in the framework of thesis co-supervisions. Two PhD students have successfully defended their thesis this year (Arash Farnam, on distributed control of lattices; Simon Apers, on quantum walks). He is further coaching a Master thesis intern working on nonlinear deterministic structures in quantum SDEs.

7.4. International Initiatives

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

TAQUILLA: is an Inria associate team (between Quantic team and Yale university) with principal Inria investigator, Mazyar Mirrahimi, and principal Yale investigator Michel Devoret. In this framework we continued our collaborations between Inria and Yale in 2018. Jérémie Guillaud visited Yale for 3 months (Sept-Nov), and Mazyar Mirrahimi for 4 months (Sept-Dec). Clarke Smith and Steven Touzard, PhD students at Yale, visited us for 1 week at the occasion of PRACQSYS meeting. Clarke Smith joins Quantic team as a postdoc in January 2019.

7.4.2. Participation in Other International Programs

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).

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- In the framework of Inria's invited professor program, Tryphon Georgiou (University of California at Irvine) visited us for about 2 months. This visit had for subject to initiate collaborations on the subject of open quantum systems and quantum channels.
- Yves Bérubé-Lauzière (University of Sherbrooke, Institut Quantique) accompanied by two PhD students made a 6-month visit from March to August 2018 to investigate with Pierre Rouchon feedback protocols for stabilizing quantum states in a high-quality cavity.
- P.S. Pereira da Silva (Escola Politécnica, PTC, University of SaoPaulo, Brazil) made a 2-week visit (June 25 to July 6) to investigate with Pierre Rouchon motion planning issues based on Lyapunov tracking for quantum gate generations.

7.5.2. Visits to International Teams

7.5.2.1. Research Stays Abroad

In the framework of our collaborations with the group of Michel Devoret at Yale university, Jérémie Guillaud and Mazyar Mirrahimi visited Yale for 3 months and 4 months, respectively, in fall 2018.

REO 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. Participation to other ANR projects

- Laurent Boudin is a member of the ANR Blanc project Kibord on kinetic models in biology and related domains
- Laurent Boudin is a member of the ANR TecSan Oxhelease
- Céline Grandmont is a member of the ANR TecSan Oxhelease
- Irene Vignon Clementel is a member of the project iLite (09/16-), RHU-santé grant, a large French hospital-medical research consortium that aims at developing innovations for liver and tissue engineering (Inria PI: Dirk Drasdo).

9.2. European Initiatives

9.2.1. Collaborations in European Programs, Except FP7 & H2020

9.2.1.1. SimInhale COST

Participant: Irene Vignon Clementel.

Action MP1404, a pan-European network of experts in the field of inhaled medicine.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

9.3.1.1. Internships

- Charu Mittal, Visiting PhD student, Indian Institute of Technology Bombay, March 2018–August 2018

RITS Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. VALET

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

Instrument: ANR

Duration: January 2016 - December 2018

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.

9.1.1.2. 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.

9.1.2. FUI

9.1.2.1. Sinetic

Title: Système Intégré Numérique pour les Transports Intelligents Coopératifs

Instrument: FUI

Duration: December 2014 - January 2018

Coordinator: Thomas Nguyen (Oktal)

Partners: Oktal, ALL4TEC, CIVITEC, Dynalogic, Inria, EURECOM, Renault, Armines, IFSTTAR, VEDECOM

Inria contact: Jean-Marc Lasgouttes

Abstract: The purpose of the project SINETIC is to create a complete simulation environment for designing cooperative intelligent transport systems with two levels of granularity: the system level, integrating all the components of the system (vehicles, infrastructure management centers, etc.) and its realities (terrain, traffic, etc.) and the component-level, modeling the characteristics and behavior of the individual components (vehicles, sensors, communications and positioning systems, etc.) on limited geographical areas, but described in detail.

9.1.2.2. PAC V2X

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

Instrument: FUI

Duration: September 2016 - August 2019

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.

9.1.3. 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). VEDECOM financed the PhD theses of Mr. Fernando Garrido and Mr. Zayed Alsayed.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. 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.

9.2.2. 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/

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. 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

9.3.2. Participation in 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.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Jean-François Lalonde from Laval University in October 2018 within the framework of Samuel de Champlain Québec-France collaboration program.

9.4.1.1. Internships

Shirsendu Halder, June-December 2018.

Nabila Arib, April-September 2018

9.4.2. Visits to International Teams

9.4.2.1. 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 BRUTUS** (10/14 → 09/18)
  Authenticated Ciphers and Resistance against Side-Channel Attacks
  ANR program: Défi Société de l'information et de la communication
  Partners: ANSSI, Inria (project-team SECRET and project-team MARELLE), Orange, University of Lille, University of Rennes, University Versailles-Saint Quentin
  160 kEuros
  The Brutus project aims at investigating the security of authenticated encryption systems. We plan to evaluate carefully the security of the most promising candidates to the CAESAR competition, by trying to attack the underlying primitives or to build security proofs of modes of operation. We target the traditional black-box setting, but also more "hostile" environments, including the hardware platforms where some side-channel information is available.
- **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** ($10/17 \rightarrow 09/21$)
  Quantum Banknotes and Information-Theoretic Credit Cards
  ANR Program: AAP Générique 2017
  Partners: Univ. Paris-Diderot (coordinator), Inria SECRET, UPMC (LIP6), CNRS (Laboratoire Kastler Brossel)
  87 kEuros
  For a quantum-safe future, classical security systems as well as quantum protocols that guarantee security against all adversaries must be deployed. Here, we will study and implement one of the most promising quantum applications, namely unforgeable quantum money. A money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or via the use of banknotes, with maximal security guarantees. Our objectives are to perform a theoretical analysis of quantum money schemes, in realistic conditions and for encodings in both discrete and continuous variables, and to demonstrate experimentally these protocols using state-of-the-art quantum memories and integrated detection devices.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PQCRYPTO

Title: Post-quantum cryptography for long-term security

Programm: H2020

Duration: March 2015 - March 2018

Coordinator: TECHNISCHE UNIVERSITEIT EINDHOVEN

Partners:

Academia Sinica (Taiwan)

Bundesdruckerei (Germany)

Danmarks Tekniske Universitet (Denmark)

Katholieke Universiteit Leuven (Belgium)

Nxp Semiconductors Belgium Nv (Belgium)

Ruhr-Universitaet Bochum (Germany)

Stichting Katholieke Universiteit (Netherlands)

Technische Universiteit Eindhoven (Netherlands)

Technische Universitaet Darmstadt (Germany)

University of Haifa (Israel)

Inria contact: Nicolas Sendrier

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

attacks accelerated by these computers. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher as Enigma-encrypted messages are today. PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things. PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

8.2.1.2. QCALL

Title: Quantum Communications for ALL

Programm: H2020-MSCA-ITN-2015

Duration: December 2016 - November 2020

Coordinator: University of Leeds (UK)

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

Inria contact: Anthony Leverrier

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

8.2.1.3. ERC QUASYModo

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

Program: ERC starting grant

Duration: September 2017 - August 2022

PI: María Naya Plasencia

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

8.2.2. Collaborations in European Programs, Except FP7 & H2020

8.2.2.1. QCDA

Program: QuantERA ERA-NET Cofund in Quantum Technologies

Project acronym: QCDA

Project title: Quantum Code Design and Architecture

Duration: February 2018 - January 2021

Coordinator: Earl Campbell, University of Sheffield, UK

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

Inria contact: Anthony Leverrier

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

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

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

8.3. International Initiatives

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

8.3.1.1. CHOCOLAT

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

International Partner (Institution - Laboratory - Researcher):

NTU (Singapore) - SYLLAB - Peyrin Thomas

Start year: 2017

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

The hash function SHA-1 is one of the most widely used hash functions in the industry, but it has been shown to not be collision-resistant by a team of Chinese researchers led by Prof. Wang in 2005. However, nobody has publicly produced a real pair of colliding messages so far, because the estimated attack complexity is around 2^{63} SHA-1 computations (this represents about 70000 years of computation on a normal PC).

While a collision of SHA-1 would clearly demonstrate the weakness of the algorithm, a much more powerful attack would be to find a collision such that the prefix of the colliding messages

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

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

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution - Laboratory - Researcher):

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

Duration: 2014 - 2018

Start year: 2014

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

8.3.2.2. Informal International Partners

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

8.4. International Research Visitors

8.4.1. Visits of International Scientists

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

8.4.1.1. Internships

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

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

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

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. National Initiatives

9.2.1. ANR

ANR HHOMM: "Hybrid high-order methods on polyhedral meshes", Theoretical foundations and applications (up to software development) for the recently-devised Hybrid high-order methods. Coordinated by D. Di Pietro, University of Montpellier. SERENA representant is A. Ern, period 2015–2019.

ANR DEDALES: "Algebraic and geometric domain decomposition for subsurface flow". The project aims at developing high performance software for the simulation of two phase flow in porous media. It specifically targets parallel computers where each node is itself composed of a large number of processing cores, such as are found in new generation many-core architectures.

The partners are HIEPACS, Laboratoire Analyse, Géométrie et Application, University Paris 13, Maison de la Simulation, and ANDRA. SERENA representants are M. Kern (grant leader) and M. Vohralík, period 2014–2018. The project ended in October 2018.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

- EoCoE: "Energy Oriented Center of Excellence" This project is coordinated by Maison de la Simulation and gathers 23 partners from 13 countries to use the tremendous potential offered by the ever-growing computing infrastructure to foster and accelerate the European transition to a reliable low carbon energy supply using HPC (High Performance Computing). SERENA representant M. Kern, period 2015–2018.
- 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), period 2015–2020.
- PRACE: "Partnership for Advanced Computing in Europe" The mission of PRACE is to enable high-impact scientific discovery and engineering research and development across all disciplines to enhance European competitiveness for the benefit of society. PRACE has an extensive education and training effort for effective use of the Research Infrastructure. M. Kern is the French representative for training, and is in charge of the French node of the Prace training network, organizing 10-12 courses each year (period 2017-2019).

9.3.2. Collaborations in European Programs, Except FP7 & H2020

OPENCPS

Program: ITEA 3

Project acronym: OPENCPS

Project title: Open cyber-physical system model-driven certified development

Duration: Dec 2015–Dec 2018

Coordinator: Magnus Eek

Other partners: AB SKF, CEA, ELTE-Soft Kft., ESI Group, EDF, Wqua Simulation AB, Ericsson, IncQuery Labs Kft., KTH, Linköping University, RTE, SICS, SIREHNA, Saab AB, Sherpa Engineering, Siemens Industrial Torbumachinery AB, VTT Technical Research Center of Finland Ltd.

Abstract: Cyber-physical systems put increasing demands on reliability, usability, and flexibility while, at the same time, lead time and cost efficiency are essential for industry competitiveness. Tools and environments for model-based development of cyber-physical systems are becoming increasingly complex and critical for the industry: tool interoperability, vendor lock-ins, and tool life-cycle support are some of the challenges. The project focuses on interoperability between the standards Modelica/UML/FMI, improved execution speed of (co-)simulation, and certified code generation.

SERENA representants are Sébastien Furic and Pierre Weis.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

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

Jean-Luc Guermond, Professor at Texas A&M University, USA, finite element methods.

Ulrich Rüde, Professor at Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany, multigrid methods.

Mary Wheeler, professor, University of Texas at Austin, USA, porous media applications.

Barbara Wohlmuth, Professor at Technical University of München, Germany, mixed finite element methods.

9.4.2. Participation in Other International Programs

Alexandre Ern participated for two weeks in Jul 2018 as an invited scientist in the ESI Program on Numerical Analysis on Complex PDE in the Sciences, Vienna, Austria (https://www.esi.ac.at/activities/events/2018/numerical-analysis-of-complex-pde-models-in-the-sciences).

9.5. International Research Visitors

9.5.1. Visits of International Scientists

Iain Smears, lecturer at University College London, March 26–30.

Thirupathi Gudi, Professor at Indian Institute of Science, Bangalore, India, January 15–February 28.

Jean-Luc Guermond, Professor at Texas A&M University, College Station, Texas, May 1–June 15.

Iain Smears, lecturer at University College London, June 18–27, and Christian Kreuzer, Professor at University Dortmund, June 18–29.

Carsten Carstensen, Professor at Humboldt University, Berlin, August 20–September 20.

Roland Becker, Professor at University of Pau, September 17–20.

Hend Ben Ameur, Professor at IPEST and member of ENIT-Lamsin, Tunis, Tunisia, November 19–30.

Théophile Chaumont-Frelet, junior researcher at Inria Sophia Antipolis, November 22–23.

9.5.1.1. Internships

Intissar Addali, 2nd year internship at ENSTA ParisTech, from May to Aug 2018, supervised by Karol Cascavita and Alexandre Ern.

9.5.2. Visits to International Teams

9.5.2.1. Research Stays Abroad

Alexandre Ern visited the research group of Prof. Victor Calo, Curtin University, Perth, Australia, in November 2018.

Martin Vohralík was invited for two weeks stay to Charles University, Prague for collaboration with J. Málek, April 2018.

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

- **ITN Spartan**
  Title: Sparse Representations and Compressed Sensing Training Network
  Type: FP7
  Instrument: Initial Training Network
  Duration: October 2014 to October 2018
  Coordinator: Mark Plumbley (University of Surrey)
  Inria contact: Francis Bach
  Abstract: The SpaRTaN Initial Training Network will train a new generation of interdisciplinary researchers in sparse representations and compressed sensing, contributing to Europe's leading role in scientific innovation. By bringing together leading academic and industry groups with expertise in sparse representations, compressed sensing, machine learning and optimisation, and with an interest in applications such as hyperspectral imaging, audio signal processing and video analytics, this project will create an interdisciplinary, trans-national and inter-sectorial training network to enhance mobility and training of researchers in this area. SpaRTaN is funded under the FP7-PEOPLE-2013-ITN call and is part of the Marie Curie Actions — Initial Training Networks (ITN) funding scheme: Project number - 607290
- **ITN Macsenet**
  Title: Machine Sensing Training Network
  Type: H2020
  Instrument: Initial Training Network
  Duration: January 2015 - January 2019
  Coordinator: Mark Plumbley (University of Surrey)
  Inria contact: Francis Bach
  Abstract: The aim of this Innovative Training Network is to train a new generation of creative, entrepreneurial and innovative early stage researchers (ESRs) in the research area of measurement and estimation of signals using knowledge or data about the underlying structure. We will develop new robust and efficient Machine Sensing theory and algorithms, together methods for a wide range of signals, including: advanced brain imaging; inverse imaging problems; audio and music signals; and non-traditional signals such as signals on graphs. We will apply these methods to real-world problems, through work with non-Academic partners, and disseminate the results of this research to a wide range of academic and non-academic audiences, including through publications, data, software and public engagement events. MacSeNet is funded under the H2020-MSCA-ITN-2014 call and is part of the Marie Sklodowska- Curie Actions — Innovative Training Networks (ITN) funding scheme.

- **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, bioin- formatics, 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 Initiatives

9.3.1. BigFOKS2

Title: Learning from Big Data: First-Order methods for Kernels and Submodular functions

International Partner (Institution - Laboratory - Researcher):

IISc Bangalore (India) - Computer Science Department - Chiranjib Bhattacharyya

Start year: 2016

See also: mllab.csa.iisc.ernet.in/indo-french.html

Recent advances in sensor technologies have resulted in large amounts of data being generated in a wide array of scientific disciplines. Deriving models from such large datasets, often known as “Big Data”, is one of the important challenges facing many engineering and scientific disciplines. In this proposal we investigate the problem of learning supervised models from Big Data, which has immediate applications in Computational Biology, Computer vision, Natural language processing, Web, E-commerce, etc., where specific structure is often present and hard to take into account with current algorithms. Our focus will be on the algorithmic aspects. Often supervised learning problems can be cast as convex programs. The goal of this proposal will be to derive first-order methods which can be effective for solving such convex programs arising in the Big-Data setting. Keeping this broad goal in mind we investigate two foundational problems which are not well addressed in existing literature. The first problem investigates Stochastic Gradient Descent Algorithms in the context of First-order methods for designing algorithms for Kernel based prediction functions on Large Datasets. The second problem involves solving discrete optimization problems arising in Submodular formulations in Machine Learning, for which first-order methods have not reached the level of speed required for practical applications (notably in computer vision).

9.4. International Research Visitors

- Vijaya Bollapragada from Northwestern University, Chicago, IL, United States, Apr - Jul 2018.
- Aaron De Fazio from Facebook Research NY, New York, United States, Feb 2018.
- Gauthier Gidel from University of Montreal - MILA, Montreal, Canada, Jan 2018.
- Sharan Vaswani from University of British Columbia, Vancouver, Canada, Apr - Jul 2018
- Simon Lacoste-Julien from University of Montreal - MILA, Montreal, Canada, Aug 2018.

VALDA Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

Michaël Thomazo has obtained a 6k€ budget from the Île-de-France region (DIM RFSI – *Réseau Francilien en Sciences Informatiques*) entitled *ISORE: Indexation sémantique d'ontologies, le cas des règles existentielles.* The grant was awarded when Michaël Thomazo was part of the Inria Saclay Cedar team, but the budget was transferred to the Valda team.

7.2. National Initiatives

7.2.1. ANR

Valda has been part of two ANR projects in 2018:

- HEADWORK (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 (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/.

In addition, two ANR projects were accepted in 2018 and will start early 2019:

- CQFD (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.
- QUID (budget managed by Inria), LIGM (coordinator), IRIF, and LaBRI, on incomplete and inconsistent data.

7.3. International Initiatives

7.3.1. IIL projects

Valda has strong collaborations with the following international groups:

Univ. Edinburgh, United Kingdom: Peter Buneman and Leonid Libkin

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

TU Dresden, Germany: Markus Krötzsch and Sebastian Rudolph

Dortmund University, Germany: Thomas Schwentick

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

National University of Singapore: Stéphane Bressan

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Victor Vianu, Professor at UC San Diego and holder of an Inria international chair, spent 3 months within Valda, employed as an ENS invited professor.

7.4.2. Visits to International Teams

7.4.2.1. Research Stays Abroad

- Michaël Thomazo and Pierre Senellart have spent respectively two weeks and one week at TU Dresden, collaborating with Markus Krötzsch and Sebastian Rudolph.
- Pierre Senellart has spent a cumulated time of around three weeks at National University of Singapore, co-advising Debabrota Basu, PhD student working under the co-supervision of Stéphane Bressan, visiting Stéphane Bressan and other researchers at NUS, and participating in the French–Singapore workshop on AI, where Olivier Cappé represented CNRS.

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 International Labs

- EPFL-Inria Lab Our work on scheduling [13] and on the Ipanema DSL [48] is done as part of the EPFL-Inria Lab. Our direct partners, Willy Zwaenepoel and Baptiste Lepers, have moved to the University of Sydney in September 2018. Therefore we have migrated our cooperation.

9.3.2. Inria International Partners

9.3.2.1. Informal International Partners

- We collaborate with David Lo and Lingxiao Jiang of Singapore Management University, who are experts in software mining, clone detection, and information retrieval techniques. Our work with Lo and/or Jiang has led to 8 joint publications since 2013 [58], [69], [71], [74], [75], [76], [79], [77], at conferences including ASE and ICSME. The ITrans ANR is a joint project with them.
- We collaborate with David Lo and James Hoang of Singapore Management University and with Sasha Levin of Microsoft on the use of machine learning to identify stable-relevant patches in the Linux kernel. Preliminary results from this collaboration have been presented with Sasha Levin at the Open Source Summit North America, the Open Source Summit Europe, and the Linux Plumbers Conference kernel summit track.
- Our previous collaboration with EPFL has been transfered to the University of Sydney due to the moves of Willy Zwaenepoel and Baptiste Lepers.
- We collaborate with Christoph Reichenbach of the University of Lund and Krishna Narasimhan of Itemis (Germany) on program transformation and the design of tools for code clone management [11].
- We collaborate with Jia-Ju Bai of Tsinghua University on bug finding in Linux kernel code, particularly focusing on issues requiring interprocedural analysis [12].
- As part of the LIP6 Invited Professor program, we have initiated a collaboration between Karine Heydeman (ALSOC team – LIP6, France) and Patrick Schaumont (Virginia Tech, US) on the development of fault-resistant and side-channel attack resistant compilation techniques.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Patrick Schaumont of Virginia Tech visited LIP6 in July and November 2018, as part of the LIP6 Invited Professor program.
- David Lo and Lingxiao Jiang of Singapore Management University visited the Whisper team for two weeks in October 2018 as part of the ANR ITrans project.
- Michele Martone of the Leibniz Supercomputing Centre in Munich Germany made two visits of one week each to the Whisper team in August and December to work on applying Coccinelle to high performance computing code.

9.4.1.1. Internships

- Jonathan Carroll of Oberlin College spent January 2018 working on using machine learning to identify stable-relevant patches for the Linux kernel.
- David Bergvelt of the University of Illinois at Urbana-Champaign spent May-August 2018 working on applying Verifiable C, developed at Princeton, to verification of process schedulers.

WILLOW Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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. European Research Council (ERC) Starting Grant: “Activia" - Ivan Laptev

Participant: Ivan Laptev.

WILLOW will be funded in part from 2013 to 2018 by the ERC Starting Grant "Activia" awarded to Ivan Laptev by the European Research Council.

‘Computer vision is concerned with the automated interpretation of images and video streams. Today’s research is (mostly) aimed at answering queries such as ’Is this a picture of a dog?’, (classification) or sometimes ’Find the dog in this photo’ (detection). While categorisation and detection are useful for many tasks, inferring correct class labels is not the final answer to visual recognition. The categories and locations of objects do not provide direct understanding of their function i.e., how things work, what they can be used for, or how they can act and react. Such an understanding, however, would be highly desirable to answer currently unsolvable queries such as ’Am I in danger?’ or ’What can happen in this scene?’. Solving such queries is the aim of this proposal. My goal is to uncover the functional properties of objects and the purpose of actions by addressing visual recognition from a different and yet unexplored perspective. The main novelty of this proposal is to leverage observations of people, i.e., their actions and interactions to automatically learn the use, the purpose and the function of objects and scenes from visual data. The project is timely as it builds upon the two key recent technological advances: (a) the immense progress in visual recognition of objects, scenes and human actions achieved in the last ten years, as well as (b) the emergence of a massive amount of public image and video data now available to train visual models. ACTIVIA addresses fundamental research issues in automated interpretation of dynamic visual scenes, but its results are expected to serve as a basis for ground-breaking technological advances in practical applications. The recognition of functional properties and intentions as explored in this project will directly support high-impact applications such as detection of abnormal events, which are likely to revolutionise today’s approaches to crime protection, hazard prevention, elderly care, and many others.’

9.2.2. European Research Council (ERC) Starting Grant: "Leap" - Josef Sivic

Participant: Josef Sivic.

The contract has begun on Nov 1st 2014. WILLOW will be funded in part from 2014 to 2018 by the ERC Starting Grant "Leap" awarded to Josef Sivic by the European Research Council.

'People constantly draw on past visual experiences to anticipate future events and better understand, navigate, and interact with their environment, for example, when seeing an angry dog or a quickly approaching car. Currently there is no artificial system with a similar level of visual analysis and prediction capabilities. LEAP is a first step in that direction, leveraging the emerging collective visual memory formed by the unprecedented amount of visual data available in public archives, on the Internet and from surveillance or personal cameras - a complex evolving net of dynamic scenes, distributed across many different data sources, and equipped with plentiful but noisy and incomplete metadata. The goal of this project is to analyze dynamic patterns in this shared visual experience in order (i) to find and quantify their trends; and (ii) learn to predict future events in dynamic scenes. With ever expanding computational resources and this extraordinary data, the main scientific challenge is now to invent new and powerful models adapted to its scale and its spatio-temporal, distributed and dynamic nature. To address this challenge, we will first design new models that generalize across different data sources, where scenes are captured under vastly different imaging conditions such as camera viewpoint, temporal sampling, illumination or resolution. Next, we will develop a framework for finding, describing and quantifying trends that involve measuring long-term changes in many related scenes. Finally, we will develop a methodology and tools for synthesizing complex future predictions from aligned past visual experiences. Our models will be automatically learnt from large-scale, distributed, and asynchronous visual data, coming from different sources and with different forms of readily-available but noisy and incomplete metadata such as text, speech, geotags, scene depth (stereo sensors), or gaze and body motion (wearable sensors). Breakthrough progress on these problems would have profound implications on our everyday lives as well as science and commerce, with safer cars that anticipate the behavior of pedestrians on streets; tools that help doctors monitor, diagnose and predict patients' health; and smart glasses that help people react in unfamiliar situations enabled by the advances from this project.'

9.3. International Initiatives

9.3.1. 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.

9.3.2. 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

Alexei Efros (Professor, UC Berkeley, USA) visited Willow during May-June. Ramazan Cinbis (Middle East Technical University) and David Fouhey (University of Michigan) visited Willow in July-August and September-November, respectively. Akihiko Torii (Tokyo Institute of Technology) spent sabbatical at Willow from Apr to August 2018. Finally, 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.