RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2019

Section Partnerships and Cooperations

Edition: 2020-03-21

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY
1. ARIC Project-Team 5
2. AROMATH Project-Team 7
3. CARAMBA Project-Team 10
4. CASCADE Project-Team 12
5. DATASHAPE Project-Team 17
6. GAMBLE Project-Team 19
7. GRACE Project-Team 23
8. LFANT Project-Team 24
9. OURAGAN Project-Team 27
10. POLSYS Project-Team 29
11. SECRET Project-Team 32
12. SPECFUN Project-Team 37
ARCHITECTURE, LANGUAGES AND COMPILATION
13. CAIRN Project-Team 38
14. CAMUS Project-Team 45
15. CASH Project-Team 47
16. CORSE Project-Team 48
17. PACAP Project-Team 50
EMBEDDED AND REAL-TIME SYSTEMS
18. HYCOMES Project-Team 54
19. Kairos Project-Team 57
20. KOPERNIC Team 60
21. PARKAS Project-Team 61
22. SPADES Project-Team 63
23. TEA Project-Team 66
PROOFS AND VERIFICATION
24. ANTIQUE Project-Team 69
25. CAMBIUM Project-Team 74
26. CELTIQUE Project-Team 75
27. CONVECS Project-Team 78
28. DEDUCTEAM Project-Team 81
29. GALLINETTE Project-Team 82
30. MEXICO Project-Team 85
31. MOCQUA Team 86
32. PARSIFAL Project-Team 88
33. PI.R2 Project-Team 89
34. STAMP Project-Team 92
35. SUMO Project-Team 94
36. TOCCATA Project-Team 98
37. VERIDIS Project-Team 101

SECURITY AND CONFIDENTIALITY

38. CIDRE Project-Team 107
39. COMETE Project-Team 109
40. DATASPHERE Team 112
41. PESTO Project-Team 113
42. PRIVATICS Project-Team 115
43. PROSECCO Project-Team 120
44. TAMIS Project-Team 125

ARIC Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR FastRelax Project

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

FastRelax stands for "Fast and Reliable Approximation". It is a four year ANR project (started in October 2014 and extended till September 2019). The web page of the project is http://fastrelax.gforge.inria.fr/. It is headed by B. Salvy and involves AriC as well as members of the Marelle Team (Sophia), of the Mac group (LAAS, Toulouse), of the Specfun and Toccata Teams (Saclay), as well as of the Pequan group in UVSQ and a colleague in the Plume group of LIP.

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

9.1.2. ANR ALAMBIC Project

Participants: Benoît Libert, Fabien Laguillaumie, Ida Tucker.

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

9.1.3. RISQ Project

Participants: Chitchanok Chuengsatiansup, Rikki Amit Inder Deo, Hervé Tale Kalachi, Fabien Laguillaumie, Benoît Libert, Damien Stehlé.

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

9.2. European Initiatives

9.2.1. PROMETHEUS Project

Participants: Fabien Laguillaumie, Benoît Libert, Octavie Paris, Damien Stehlé.

PROMETHEUS (Privacy-Preserving Systems from Advanced Cryptographic Mechanisms Using Lattices) is a 4-year European H2020 project (call H2020-DS-2016-2017, Cybersecurity PPP Cryptography, DS-06-2017) that started in January 2018. It gathers 8 academic partners (ENS de Lyon and Université de Rennes 1; CWI, Pays-Bas; IDC Herzliya, Israel; Royal Holloway University of London, United Kingdom; Universitat Politècnica de Catalunya, Spain; Ruhr-Universität Bochum, Germany; Weizmann Institute, Israel), 4 industrial partners (Orange, Thales, TNO, Scytl). The goal of this project is to develop a toolbox of privacy-preserving cryptographic algorithms and protocols (like group signatures, anonymous credentials, or digital cash systems) that resist quantum adversaries. Solutions will be mainly considered in the context of Euclidean lattices and they will be analyzed from a theoretical point of view (i.e., from a provable security aspect) and a practical angle (which covers the security of cryptographic implementations and side-channel leakages). The project is hosted by ENS de Lyon and Benoît Libert is the administrative coordinator while Orange is the scientific leader.

9.3. International Initiatives

9.3.1. Participation in Other International Programs

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

Participants: Benoît Libert, Damien Stehlé.

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

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

9.3.1.2. Inria International Chairs

- **TUCKER Warwick**
- Department of Mathematics - Uppsala University - Sweden
- Title: Attracteur de Hénon et intégrales abéliennes liées aux 16e problème de Hilbert
- 2018 – 2022

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Ron Steinfeld, Monash University (June)
- Amin Sakzad, Monash University (June)
- Shi Bai, Florida Atlantic University (June and July)
- David Wu, University of Virginia (July)
- Olivier Bernard, Université Rennes 1 and Thalès (October and November)
- Gautier Eberhart, Université Rennes 1 (October and November)
- Federico Savasta, Università degli Studi di Catania (October)

AROMATH Project-Team

7. Partnerships and Cooperations

7.1. European Initiatives

7.1.1. FP7 & H2020 Projects

7.1.1.1. ARCADES

Program: Marie Skłodowska-Curie ETN

Project acronym: ARCADES

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

Duration: January 2016 - December 2019

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

Scientist-in-charge at Inria: L. Busé

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

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

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

7.1.1.2. POEMA

Program: Marie Skłodowska-Curie ITN

Project acronym: POEMA

Project title: Polynomial Optimization, Efficiency through Moments and Algebra

Duration: January 2019 - December 2022 (48 months)

Coordinator: B. Mourrain (Aromath, Inria Sophia Antipolis)

Other partners: LAAS - CNRS, Toulouse (France), Sorbonne Université, Paris (France), Centrum Wiskunde & Informatica, Amsterdam (The Netherlands), Stichting Katholieke Universiteit Brabant, Tilburd (The Netherlands), Universität Konstanz (Germany), Università degli Studi di Firenze (Italy), University of Birmingham (United Kingdom), Friedrich Alexander University Erlangen-Nuremberg (Germany), Universitet I Tromsø (Norway), ARTELYS SAS, Paris (France).

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

Abstract: Non-linear optimization problems are present in many real-life applications and in scientific areas such as operations research, control engineering, physics, information processing, economy, biology, etc. However, efficient computational procedures, that can provide the guaranteed global optimum, are lacking for them. The project will develop new polynomial optimization methods, combining moment relaxation procedures with computational algebraic tools to address this type of problems. Recent advances in mathematical programming have shown that the polynomial optimization problems can be approximated by sequences of Semi-Definite Programming problems. This approach provides a powerful way to compute global solutions of non-linear optimization problems and to guarantee the quality of computational results. On the other hand, advanced algebraic algorithms to compute all the solutions of polynomial systems, with efficient implementations for exact and approximate solutions, were developed in the past twenty years. The network combines the expertise of active European teams working in these two domains to address important challenges in polynomial optimization and to show the impact of this research on practical applications.

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

7.1.1.3. GRAPES

Program: Marie Skłodowska-Curie ETN

Project acronym: GRAPES

Project title: Learning, Processing and Optimising Shapes

Duration: December 2019 - November 2023

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

Scientist-in-charge at Inria: L. Busé

Other partners: U. Barcelona (Spain), Inria Sophia-Antipolis (France), J. Kepler University, Linz (Austria), SINTEF Institute, Oslo (Norway), U. Strathclyde, Glascow (UK), RWTH Aachen (Germany), U. Svizzera Italiana (Switzerland), U. Tor Vergata (Italy), Vilnius U. (Lithuania), GeometryFactory SARL (France).

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

Abstract: GRAPES aims at advancing the state of the art in Mathematics, Computer-Aided Design, and Machine Learning in order to promote game changing approaches for generating, optimising, and learning 3D shapes, along with a multisectoral training for young researchers. Recent advances in the above domains have solved numerous tasks concerning multimedia and 2D data. However, automation of 3D geometry processing and analysis lags severely behind, despite their importance in science, technology and everyday life, and the well-understood underlying mathematical principles. GRAPES spans the spectrum from Computational Mathematics, Numerical Analysis, and Algorithm Design, up to Geometric Modelling, Shape Optimisation, and Deep Learning. This allows the 15 PhD candidates to follow either a theoretical or an applied track and to gain knowledge from both research and innovation through a nexus of intersectoral secondments and Network-wide workshops. Horizontally, our results lead to open-source, prototype implementations, software integrated into commercial libraries as well as open benchmark datasets. These are indispensable for dissemination and training but also to promote innovation and technology transfer. Innovation relies on the active participation of SMEs, either as a beneficiary hosting an ESR or as associate partners hosting secondments. Concrete applications include simulation and fabrication, hydrodynamics and marine design, manufacturing and 3D printing, retrieval and mining, reconstruction and visualisation, urban planning and autonomous driving.

7.2. International Initiatives

7.2.1. Participation in Other International Programs

7.2.1.1. PHC Alliance

- Program: PHC Alliance
- Project title: High-order methods for computational design and data-driven engineering
- Duration: 01/2020–12/2021
- Coordinator: Angelos Mantzaflaris
- Other partners: Swansea University, UK
- Abstract: The aim of this project is to develop a mathematical framework for the integration of geometric modeling and simulation using spline-based finite elements of high degree of smoothness. High-order methods are known to provide a robust and efficient methodology to tackle complex challenges in multi-physics simulations, shape optimization, and the analysis of large-scale datasets arising in data-driven engineering and design. However, the analysis and design of high-order methods is a daunting task requiring a concurrent effort from diverse fields such as applied algebraic geometry, approximation theory and splines, topological data analysis, and computational mathematics. Our strategic vision is to create a research team combining a uniquely broad research expertise in these areas by establishing a link between the team AROMATH at Inria Sophia-Antipolis and Swansea University.

7.2.1.2. NSFC

- Program: NSFC
- Project title: "Research on theory and method of time-varying parameterization for dynamic isogeometric analysis",
- Duration: 2018-2021.
- Collaboration project with Gang Xu, Hangzhou Dianzi University, China.

7.3. International Research Visitors

7.3.1. Visits of International Scientists

Gang Xu, Hangzhou Dianzi University, China, visited AROMATH team (9 - 20 Oct.) to work on Isogeometric Analysis and Geometric Modeling.

Ibrahim Adamou, Univ. Dan Dicko Dankoulodo de Maradi, Niger, visited B. Mourrain (28 Oct. - 21 Dec.) to work on medial axes of curve arcs.

7.3.1.1. Internships

Martin Jalard (L3, Ecole normale supérieure de Rennes) for his *introduction to research* internship explored during 6 weeks (May 13th to June 21st) the application of Norton's lemma to the computation of isotypic decompositions.

7.3.2. Visits to International Teams

7.3.2.1. Research Stays Abroad

Evelyne Hubert was awarded a Simons fellowship within the program *Geometry, compatibility and structure preservation in computational differential equations*, from July to December 2019, at the Isaac Newton Institute in Cambridge (UK).

For the month of April, Evelyne Hubert was a guest professor a the University of the Arctic for *Pure Mathematics in Norway*.

Angelos Mantzaflaris visited in April the Computational Foundry, Swansea University, UK in the frame of the College of Science International Visitor Scheme.

CARAMBA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. CPER CyberEntreprises

Program: CPER (Contrat de Plan État Région)

Project title: Cyber-Entreprises

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

Coordinator: Emmanuel Thomé and Marc Jungers (CRAN)

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

Abstract: cf web site (in French only).

A high-performance computer cluster was funded by the CPER Cyber-entreprises project (Région Grand-Est, French Ministry of Research and Higher Education, Inria, CNRS). This cluster is also mentioned in 6.3 .

9.2. National Initiatives

9.2.1. FUI Industrial Partnership on Lightweight Cryptography

Program: FUI (Fonds Unique Interministériel)

Project acronym: PACLIDO

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

Duration: 12/2017 - 12/2020

Coordinator: Airbus Cybersecurity

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

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

9.2.2. ANR Decrypt

The CARAMBA team coordinates this ANR Project (started in January 2019) with the 5 following partners: LORIA, LIRIS (Lyon), LIMOS (Clermont-Ferrand), IRISA (Rennes), TASC (Nantes). This project aims to propose a declarative language dedicated to cryptanalytic problems in symmetric key cryptography using constraint programming (CP) to simplify the representation of attacks, to improve existing attacks and to build new cryptographic primitives that withstand these attacks. We also want to compare the different tools that can be used to solve these problems: SAT and MILP where the constraints are homogeneous and CP where the heterogeneous constraints can allow a more complex treatment.

One of the challenges of this project will be to define global constraints dedicated to the case of symmetric cryptography.

Concerning constraint programming, this project will define new dedicated global constraints, will improve the underlying filtering and solution search algorithms, and will propose dedicated explanations generated automatically. This 4-year project started in January 2019. See web site for more information.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Diego Aranha from Aarhus University visited the team one week in May and presented his work on the Brazilian voting machines at the SSL seminar, and his work on fast pairing implementation at the team's seminar. As a result, some of the new secure pairing-friendly curves of [21], [22] are implemented in the C++ library RELIC [0] (free software).
- Santanu Sarkar from IIT Madras, Chennai, India is visiting the team from December 2019 to the end of February 2020.

9.3.1.1. Internships

- Hamid Boukerrou (Université Paris 8, from March 2019 until September 2019). Subject: cryptanalysis of LBlock.
- Félix Breton (ÉNS Paris, from June 2019 until July 2019). Félix Breton has formally proven in Coq the GNU MPFR subtraction routine in the case where all three operands (the two inputs and the result) have the same precision p, and $1 \leq p < w$, where w is the machine bit-size. This extends previous work done by Jianyang Pan in 2018 on the addition and multiplication routines.
- Émilien Failly (CPP Nancy, from April 2019 until June 2019). Émilien Failly studied the Multiple Polynomial General Number Field Sieve (MNFS). He compared the use of 2, 3, and 4 polynomials on three test numbers: a 60-digit number, a 70-digit number, and a 96-digit number. In each case, the sieving time was estimated, because Cado-NFS cannot currently fully deal with MNFS polynomials.
- Liwei Liu (Peking University, from June 2019 until September 2019). In the context of the computation of discrete logarithms in finite field extensions of small degree, using the Number Field Sieve, Liwei Liu worked on the individual logarithm step, in order to make it faster and more robust.
- Rémi Piau (ÉNS Rennes, from May 2019 until July 2019). Rémi Piau worked on the implementation in Python of our attack against ECDSA using wNAF representation. He was able to improve it by making it cleaner, and using small tricks to make it faster too.

[0] https://github.com/relic-toolkit/relic

CASCADE Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives with Industry

7.1.1. ANBLIC: Analysis in Blind Clouds

Program: FUI

Duration: January 2018 – December 2020

Coordinator: Wallix

Partners: UPEC, CEA, Atos, SOGETI, CoeSSI

Local coordinator: David Pointcheval

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

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

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

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

Program: GDN

Duration: February 2017 – September 2020

Coordinator: Secure-IC

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

Local coordinator: Michel Abdalla and Phong Nguyen since September 2019

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

7.2. National Collaborations with Academics

7.2.1. EnBiD: Encryption for Big Data

Program: ANR JCJC

Duration: October 2014 – September 2019

PI: Hoeteck Wee

Partners: Université Paris 2, Université Limoges

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

7.2.2. EfTrEC: Efficient Transferable E-Cash

Program: ANR JCJC

Duration: October 2016 – December 2019

PI: Georg Fuchsbauer

Partners: Université Paris 2

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

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

7.2.3. SaFED: Safe and Functional Encrypted Databases

Program: ANR JCJC

Duration: October 2019 – Septembre 2023

PI: Brice Minaud

Partners: ENS, DGA

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

7.2.4. ALAMBIC: AppLicAtions of MalleaBIlity in Cryptography

Program: ANR PRC

Duration: October 2016 – September 2020

PI: Damien Vergnaud

Partners: ENS Lyon, Université Limoges

The main objectives of the proposal are the following:

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

7.3. European Initiatives

7.3.1. CryptoCloud: Cryptography for the Cloud

Program: FP7 ERC Advanced Grant

Duration: June 2014 – May 2020

PI: David Pointcheval

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

7.3.2. SAFEcrypto: Secure Architectures of Future Emerging Cryptography

Program: H2020

Duration: January 2015 – January 2019

Coordinator: The Queen's University of Belfast

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

Local coordinator: Michel Abdalla

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

7.3.3. ECRYPT-NET: Advanced Cryptographic Technologies for the Internet of Things and the Cloud

Program: H2020 ITN

Duration: March 2015 – February 2019

Coordinator: KU Leuven (Belgium)

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

Local coordinator: Michel Abdalla

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

7.3.4. aSCEND: Secure Computation on Encrypted Data

Program: H2020 ERC Starting Grant

Duration: June 2015 – May 2021

PI: Hoeteck Wee

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

7.3.5. FENTEC: Functional Encryption Technologies

Program: H2020

Duration: January 2018 – December 2020

Coordinator: ATOS Spain SA

Scientific coordinator: Michel Abdalla

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

Local coordinator: Michel Abdalla

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

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

7.4. International Initiatives with Industry

7.4.1. CryptBloC: Cryptography for the Blockchain

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

Duration: October 2017 – October 2021

PI: Georg Fuchsbauer

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

7.5. International Research Visitors

7.5.1. Professors

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

7.5.2. PhD students

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

7.6. Internships

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

DATASHAPE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

Mini course on “Sheaf Theory and Topological Data Analysis” taught by Rodrigo Cordoniu (Nice University) at Inria Sophia Antipolis — 8 weeks, 2h per week, Feb 2019 to Apr 2019.

7.2. National Initiatives

7.2.1. ANR

7.2.1.1. ANR ASPAG

Participant: Marc Glisse.

- Acronym : ASPAG.

- Type : ANR blanc.

- Title : Analysis and Probabilistic Simulations of Geometric Algorithms.

- Coordinator : Olivier Devillers (équipe Inria Gamble).

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

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

- Abstract:

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

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

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

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

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

7.3. International Research Visitors

7.3.1. Visits of International Scientists

- Arijit Ghosh, Indian Statistical Institute, Kolkata, India (September 2019)
- Ramsay Dyer Berkeley Publishing (September 2019)
- Mathijs Wintraecken, IST Austria (September and October 2019)

7.3.1.1. Internships

- Alex Delalande, Centrale-Supelec, (May-October 2019).

7.3.1.2. Research Stays Abroad

- Martin Royer, Fujitsu Laboratories, Tokyo, 2 months.

GAMBLE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR SoS

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

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

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

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

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

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

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

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

9.1.2. ANR Aspag

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

Participants:

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

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

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

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

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

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

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

9.1.3. ANR MinMax

Project title: MIN-MAX
Duration: 4 years
Starting date: 2019
Coordinator: Stéphane Sabourau (Université Paris-Est Créteil)
Participants:

- Université Paris Est Créteil, Laboratoire d'Analyse et de Mathématiques Appliquées (LAMA). Local coordinator: Stéphane Sabourau
- Université de Tours, Institut Denis Poisson. Local coordinator: Laurent Mazet. This node includes two participants from Nancy, Benoît Daniel (IECL) and Xavier Goaoc (Loria, GAMBLE).

Abstract: The MinMax projet is funded by ANR under number ANR-19-CE40-0014

This collaborative research project aims to bring together researchers from various areas – namely, geometry and topology, minimal surface theory and geometric analysis, and computational geometry and algorithms – to work on a precise theme around min-max constructions and waist estimates.

9.1.4. Institut Universitaire de France

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

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

9.2. International Initiatives

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

9.2.1.1. TRIP

Title: Triangulation and Random Incremental Paths

International Partner (Institution - Laboratory - Researcher):

Carleton University (Canada) - CGLab - Prosenjit Bose

Start year: 2018

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

The two teams are specialists of Delaunay triangulation with a focus on computation algorithms on the French side and routing on the Canadian side. We plan to attack several problems where the two teams are complementary:

- Stretch factor of the Delaunay triangulation in 3D.
- Probabilistic analysis of Theta-graphs and Yao-graphs.
- Smoothed analysis of a walk in Delaunay triangulation.
- Walking in/on surfaces.
- Routing un non-Euclidean spaces.

9.2.1.2. Astonishing

Title: ASsociate Team On Non-ISH euclIdeaN Geometry

International Partner (Institution - Laboratory - Researcher):

University of Groningen (Netherlands) - Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence - Gert Vegter

Start year: 2017

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

Some research directions in computational geometry have hardly been explored. The spaces in which most algorithms have been designed are the Euclidean spaces $\mathbb{R}^d$. To extend further the scope of applicability of computational geometry, other spaces must be considered, as shown by the concrete needs expressed by our contacts in various fields as well as in the literature. Delaunay triangulations in non-Euclidean spaces are required, e.g., in geometric modeling, neuromathematics, or physics. Topological problems for curves and graphs on surfaces arise in various applications in computer graphics and road map design. Providing robust implementations of these results is a key towards their reusability in more applied fields. We aim at studying various structures and algorithms in other spaces than $\mathbb{R}^d$, from a computational geometry viewpoint. Proposing algorithms operating in such spaces requires a prior deep study of the mathematical properties of the objects considered, which raises new fundamental and difficult questions that we want to tackle.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Gert Vegter (University of Groningen, NL) spent two weeks in GAMBLE in the context of the Astonishing associate team.

Matthijs Ebbens (University of Groningen, NL) spent one week in GAMBLE in the context of the Astonishing associate team.

Hugo Parlier (University of Luxembourg) spent two days in GAMBLE in the context of the ANR project SoS.

Erin Wolf Chambers (Saint Louis University, USA) spent two days in GAMBLE

Vanessa Robins (Australian National University) spent two days in GAMBLE

Andreas Holmsen (KAIST, South Korea) and Zuzanna Patáková (IST Austria, Vienna) spent a week in GAMBLE

9.3.2. Visits to International Teams

Olivier Devillers and Monique Teilaud spent one week in June at the Computational Geometry Lab of Carleton University http://cglab.ca/ in the context of the TRIP associate team.

Vincent Despré spent a total of three week during 2019 at the Mathematical Research Unit of the University of Luxembourg in the context of the ANR SoS project.

Sylvain Lazard spent two weeks in September at the Computational Geometry Lab of Carleton University http://cglab.ca/ in the context of the TRIP associate team.

Monique Teillaud spent two weeks at Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence of the University of Groningen in the context of the Astonishing associate team.

Monique Teillaud spent two days at University of Luxembourg in the context of the ANR SoS project

Xavier Goaoc spent one week at UNAM Queretaro, in Mexico.

GRACE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Daniel Augot, Matthieu Rambaud.

Daniel Augot and Matthieu Rambaud (Institut Mines-Telecom) received a Digicosme Grant, to fund a new PhD student, A. Saadeh, starting November 2019, on the topic of Secure Multiparty Computation.

8.2. National Initiatives

8.2.1. ANR MANTA

Participants: Daniel Augot, Alain Couvreur, Françoise Levy-Dit-Vehel, Philippe Lebacque, Matthieu Rambaud, Isabella Panaccione, Luca de Feo.

MANTA (accepted July 2015, starting March 2016, Ended September 2019): "Curves, surfaces, codes and cryptography". This project deals with applications of coding theory error correcting codes to in cryptography, multi-party computation, and complexity theory, using advanced topics in algebraic geometry and number theory.

We have four annual national retreats, the last one in January 2019, and we organized a closing international workshop in August 2019, with more than 40 participants, half French, half international.

See http://anr-manta.inria.fr/.

8.2.2. ANR CIAO

Participants: Benjamin Smith, Luca de Feo, Antonin Leroux, Mathilde de La Morinerie.

ANR **CIAO** (Cryptography, Isogenies, and Abelian varieties Overwhelming) is a JCJC 2019 project, led by Damien Robert (Inria EP LFANT). This project, which started in October 2019, will examine applications of higher-dimensional abelian varieties in isogeny-based cryptography.

8.2.3. ANR CBCRYPT

Participant: Alain Couvreur.

ANR **CBCRYPT** (Code–based Cryptography) This is a project from (*Appel à projets générique, Défi 9, Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents, Axe 4 ; Cybersécurité*). This project, starting in october 2017 led by Jean-Pierre Tillich (Inria, EP Cosmiq) focusses on the design and the security analysis of code–based primitives, in the context of the current NIST competition.

8.3. European Initiatives

8.3.1. FP7 & H2020 Projects

Participant: Benjamin Smith.

- SPARTA https://www.sparta.eu/ is a cybersecurity competence network, with the objective to collaboratively develop and implement top-tier research and innovation actions

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Alessandro Neri visited us from September 2019 to December 2019, as post-doctoral visitor, to work on rank-metric codes.
- Vincent Neiger (Mcf, Univ. Limoges) visited our team twice. One week in march and one meek in november, to work on the decoding of Reed–Solomon codes.

LFANT Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography

Participant: Guilhem Castagnos.

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

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

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

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

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

Participants: Xavier Caruso, Jean-Marc Couveignes.

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

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

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

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

7.1.3. ANR Ciao – Cryptography, Isogenies and Abelian varieties Overwhelming

Participants: Jean-Marc Couveignes, Jean Kieffer, Aurel Page, Damien Robert.

The CIAO ANR project is a young researcher ANR project led by Damien Robert October 2019.

The aim of the CIAO project is to study the security and improve the efficiency of the SIDH (supersingular isogenies Diffie Helmann) protocol, which is one of the post-quantum cryptographic project submitted to NIST, which passed the first round selection.

The project include all aspects of SIDH, from theoretical ones (computing the endomorphism ring of supersingular elliptic curves, generalisation of SIDH to abelian surfaces) to more practical aspects like arithmetic efficiency and fast implementations, and also extending SIDH to more protocols than just key exchange.

Applications of this project is to improve the security of communications in a context where the currently used cryptosystems are vulnerable to quantum computers. Beyond post-quantum cryptography, isogeny based cryptosystems also allow to construct new interesting cryptographic tools, like Verifiable Delay Functions, used in block chains.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2019

Coordinator: Nicolas Thiéry

Inria contact: Karim Belabas

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

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

7.3. International Initiatives

7.3.1. Inria International Labs

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

7.3.1.1. FAST

Title: (Harder Better) FAster STronger cryptography

International Partner (Institution - Laboratory - Researcher): and the PRMAIS project

Université des Sciences et Techniques de Masuku (Gabon) - Tony Ezome

Start year: 2017

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

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

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

This was the last year of the Fast projet, which was represented at the Journees du Lirimia in Yaounde by Emmanuel Fouotsa.

In total the project funded one EMA and two CIMPA schools, had 14 publications in journals and conferences (with three upcoming preprints), two PhD defense with two upcoming.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

The team is used to collaborating with Leiden University through the ALGANT programme for joint PhD supervision.

Eduardo Friedman (U. of Chile), long term collaborator of K. Belabas's and H. Cohen's, is a regular visitor in Bordeaux (about 1 month every year).

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Researchers visiting the team to give a talk to the team seminar include David Lubicz (DGA Rennes), Hartmut Monien (Bethe Center for Theoretical Physics, Bonn), Francesco Battestoni (University of Milan), David Roe (MIT, Boston), Maria Dostert (EPFL, Lausanne), and Alice Pellet-Mary (KU Leuven).

Abdoulaye Maiga visited the team for one month in December 2019, and Tony Ezome visited for two weeks in November 2019.

OURAGAN Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

- FMJH Program, PGMO grant

  ALMA (Algebraic methods in games and optimization).

  Duration: 2018 – 2020. (2 years project)

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

9.1.1. ANR

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

  Coordinator: Elias Tsigaridas

  Duration: 2018 – 2022

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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

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

Project acronym: Almacrypt

Project title: Algorithmic and Mathematical Cryptology

Duration: 01/2016 - 12/2010

Coordinator: Antoine Joux

Abstract: Cryptology is a foundation of information security in the digital world. Today's internet is protected by a form of cryptography based on complexity theoretic hardness assumptions. Ideally, they should be strong to ensure security and versatile to offer a wide range of functionalities and allow efficient implementations. However, these assumptions are largely untested and internet security could be built on sand. The main ambition of Almacrypt is to remedy this issue by challenging the assumptions through an advanced algorithmic analysis. In particular, this proposal questions the two pillars of public-key encryption: factoring and discrete logarithms. Recently, the PI contributed to show that in some cases, the discrete logarithm problem is considerably weaker than previously assumed. A main objective is to ponder the security of other cases of the discrete logarithm problem, including elliptic curves, and of factoring. We will study the generalization of the recent techniques and search for new algorithmic options with comparable or better efficiency. We will also study hardness assumptions based on codes and subset-sum, two candidates for post-quantum cryptography. We will consider the applicability of recent algorithmic and mathematical techniques to the resolution of the corresponding putative hard problems, refine the analysis of the

algorithms and design new algorithm tools. Cryptology is not limited to the above assumptions: other hard problems have been proposed to aim at post-quantum security and/or to offer extra functionalities. Should the security of these other assumptions become critical, they would be added to Almacrypt's scope. They could also serve to demonstrate other applications of our algorithmic progress. In addition to its scientific goal, Almacrypt also aims at seeding a strengthened research community dedicated to algorithmic and mathematical cryptology.

9.3. International Initiatives

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

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

  Duration: 2019 – 2020 (2 years project)

  Coordinator: Elias Tsigaridas

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

9.3.1.1. MACAO

Title: Mathematics and Algorithms for Cryptographic Advanced Objects

International Partner (Institution - Laboratory - Researcher):

University of Wollongong (Australia) - Thomas Plantard

Start year: 2019

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

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

9.3.2. Inria International Partners

9.3.2.1. Declared Inria International Partners

- University of Wollongong (Australia)

9.3.2.2. Informal International Partners

- CQT Singapour (UMI CNRS Majulab)
- UFPA - Para -Brésil (José Miguel Veloso)
- Institut Joseph Fourier - Université Grenoble Alpes (Martin Deraux, V. Vitse et Pierre Will)
- Max-Planck-Institut für Informatik - Saarbrücken - Germany (Alex. Kobel)
- Holon Institute of Technology, Israel (Jeremy Kaminsky)
- Department of Informatics, National Kapodistrian University of Athens, Greece (Ioannis Emiris)

POLSYS Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

  COMPUTER ALGEBRA METHODS FOR SEMI-ALGEBRAIC PROGRAMMING

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

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

8.2. National Initiatives

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

  `Duration:` 2018–2022

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

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

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

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

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

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

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

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

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

  `Duration:` 2018–2022

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

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

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

  `Duration:` 2020–2024

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

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

- **ANR DRN (DeRerumNatura)**

  `Duration:` 2020–2024

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

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

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

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

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

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

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

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

8.3. European Initiatives

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

  `Duration:` 2019–2023

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

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

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

SECRET Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- **ANR DEREC** (10/16 → 09/21)
  Relativistic cryptography
  ANR Program: jeunes chercheurs
  244 kEuros
  The goal of project DEREC is to demonstrate the feasibility of guaranteeing the security of some cryptographic protocols using the relativistic paradigm, which states that information propagation is limited by the speed of light. We plan to study some two party primitives such as bit commitment and their security against classical and quantum adversaries in this model. We then plan to the integration of those primitives into larger cryptosystems. Finally, we plan on performing a demonstration of those systems in real life conditions.
- **ANR CBCRYPT** (10/17 → 09/21)
  Code-based cryptography
  ANR Program: AAP Générique 2017
  Partners: Inria SECRET (coordinator), XLIM, Univ. Rouen, Univ. Bordeaux.
  197 kEuros
  The goal of CBCRYPT is to propose code-based candidates to the NIST call aiming at standardizing public-key primitives which resist to quantum attacks. These proposals are based either on code-based schemes relying on the usual Hamming metric or on the rank metric. The project does not deal solely with the NIST call. We also develop some other code-based solutions: these are either primitives that are not mature enough to be proposed in the first NIST call or whose functionalities are not covered by the NIST call, such as identity-based encryption, broadcast encryption, attribute based encryption or functional encryption. A third goal of this project is of a more fundamental nature: namely to lay firm foundations for code-based cryptography by developing thorough and rigorous security proofs together with a set of algorithmic tools for assessing the security of code-based cryptography.
- **ANR quBIC** (10/17 → 09/21)
  Quantum Banknotes and Information-Theoretic Credit Cards
  ANR Program: AAP Générique 2017
  Partners: Univ. Paris-Diderot (coordinator), Inria SECRET, UPMC (LIP6), CNRS (Laboratoire Kastler Brossel)
  87 kEuros
  For a quantum-safe future, classical security systems as well as quantum protocols that guarantee security against all adversaries must be deployed. Here, we will study and implement one of the most promising quantum applications, namely unforgeable quantum money. A money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or via the use of banknotes, with maximal security guarantees. Our objectives are to perform a theoretical analysis of quantum money schemes, in realistic conditions and for encodings in both discrete and continuous variables, and to demonstrate experimentally these protocols using state-of-the-art quantum memories and integrated detection devices.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. QCALL

Title: Quantum Communications for ALL

Programm: H2020-MSCA-ITN-2015

Duration: December 2016 - November 2020

Coordinator: University of Leeds (UK)

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

Inria contact: Anthony Leverrier

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

8.2.1.2. ERC QUASYModo

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

Program: ERC starting grant

Duration: September 2017 - August 2022

PI: María Naya Plasencia

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

8.2.1.3. H2020 FET Flagship on Quantum Technologies - CiViQ

Title: CiViQ *Continuous Variable Quantum Communications*

Program: H2020 FET Flagship on Quantum Technologies

Duration: October 2018 - September 2021

PI: Anthony Leverrier

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

8.2.2. Collaborations in European Programs, Except FP7 & H2020

8.2.2.1. QCDA

Program: QuantERA ERA-NET Cofund in Quantum Technologies

Project acronym: QCDA

Project title: Quantum Code Design and Architecture

Duration: February 2018 - January 2021

Coordinator: Earl Campbell, University of Sheffield, UK

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

Inria contact: Anthony Leverrier

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

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

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

8.3. International Initiatives

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

8.3.1.1. CHOCOLAT

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

International Partner (Institution - Laboratory - Researcher):

NTU (Singapore) - SYLLAB - Peyrin Thomas

Start year: 2017

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

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

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

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

8.3.2. Inria International Partners

8.3.2.1. Declared Inria International Partners

Title: Discrete Mathematics, Codes and Cryptography

International Partner (Institution - Laboratory - Researcher):

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

Duration: 2014 - 2019

Start year: 2014

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

8.3.2.2. Informal International Partners

- Nanyang Technological University (Singapore): cryptanalysis of symmetric primitives.
- Ruhr-Universität Bochum (Germany): design and cryptanalysis of symmetric primitives.
- NTT Secure Platforms Laboratories (Japan): quantum cryptanalysis, symmetric cryptography.
- University of Sherbrooke (Canada): quantum codes.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

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

8.4.1.1. Internships

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

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

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

SPECFUN Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- *De rerum natura*. This project, set up by the team, was accepted this year and will be funded until 2023. It gathers over 20 experts from four fields: computer algebra; the Galois theories of linear functional equations; number theory; combinatorics and probability. Our goal is to obtain classification algorithms for number theory and combinatorics, particularly so for deciding irrationality and transcendence.

7.1.2. Research in Pairs

Alin Bostan together with Marc Mezzaroba (CNRS, Sorbonne Université) and Tanguy Rivoal (CNRS, Université Grenoble-Alpes) have done a "research in pairs" on the Fast Computation of Values of D-Finite Functions, from December 2 to 6, 2019, at CIRM (Luminy, France). The aim of the joint project was to investigate the implications of arithmetic properties of linear differential equations on the computational complexity of their numerical solutions. They focussed on E- and G-functions, which are power series solutions of differential equations that additionally satisfy strong arithmetic conditions and play a major role in Diophantine approximation. The main goal for this research session was to understand several remarks, given without proof by Chudnovsky and Chudnovsky in the late 1980s, and stating that number-theoretic properties could lead to slightly better complexity bounds for E- and G-functions than in the general case.

7.2. International Research Visitors

7.2.1. Visits of International Scientists

7.2.1.1. Internships

- Pierre Lairez supervised during two months Abhijit Balachandra, M1-level student from the Indian Institute of Science (Bangalore). They studied some new aspects of the numerical computation of the topology of complex algebraic surfaces.

CAIRN Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Labex CominLabs - BBC (2016-2020)

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

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

7.2. National Initiatives

7.2.1. ANR AdequateDL

Participants: Olivier Sentieys, Silviu-Ioan Filip.

Program: ANR PRC

Project acronym: AdequateDL

Project title: Approximating Deep Learning Accelerators

Duration: Jan. 2019 - Dec. 2022

Coordinator: Cairn

Other partners: INL, CAIRN, LIRMM, CEA-LIST

The design and implementation of convolutional neural networks for deep learning is currently receiving a lot of attention from both industrials and academics. However, the computational workload involved with CNNs is often out of reach for low power embedded devices and is still very costly when run on datacenters. By relaxing the need for fully precise operations, approximate computing substantially improves performance and energy efficiency. Deep learning is very relevant in this context, since playing with the accuracy to reach adequate computations will significantly enhance performance, while keeping quality of results in a user-constrained range. AdequateDL will explore how approximations can improve performance and energy efficiency of hardware accelerators in deep-learning applications. Outcomes include a framework for accuracy exploration and the demonstration of order-of-magnitude gains in performance and energy efficiency of the proposed adequate accelerators with regards to conventional CPU/GPU computing platforms.

7.2.2. ANR RAKES

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

Program: ANR PRC

Project acronym: RAKES

Project title: Radio Killed an Electronic Star: speed-up parallel programming with broadcast communications based on hybrid wireless/wired network on chip

Duration: June 2019 - June 2023

Coordinator: TIMA

Other partners: TIMA, CAIRN, Lab-STICC

The efficient exploitation by software developers of multi/many-core architectures is tricky, especially when the specificities of the machine are visible to the application software. To limit the dependencies to the architecture, the generally accepted vision of the parallelism assumes a coherent shared memory and a few, either point to point or collective, synchronization primitives. However, because of the difference of speed between the processors and the main memory, fast and small dedicated hardware controlled memories containing copies of parts of the main memory (a.k.a caches) are used. Keeping these distributed copies up-to-date and synchronize the accesses to shared data, requires to distribute and share information between some may if not all the nodes. By nature, radio communications provide broadcast capabilities at negligible latency, they have thus the potential to disseminate information very quickly at the scale of a circuit and thus to be an opening for solving these issues. In the RAKES project, we intend to study how wireless communications can solve the scalability of the abovementioned problems, by using mixed wired/wireless Network on Chip. We plan to study several alternatives and to provide (a) a virtual platform for evaluation of the solutions and (b) an actual implementation of the solutions.

7.2.3. ANR Opticall^2

Participants: Olivier Sentieys, Cédric Killian, Daniel Chillet.

Program: ANR PRCE

Project acronym: Opticall^2

Project title: on-chip OPTIcal interconnect for ALL to ALL communications

Duration: Dec. 2018 - Nov. 2022

Coordinator: INL

Other partners: INL, CAIRN, C2N, CEA-LETI, Kalray

The aim of Opticall^2 is to design broadcast-enabled optical communication links in manycore architectures at wavelengths around 1.3μm. We aim to fabricate an optical broadcast link for which the optical power is equally shared by all the destinations using design techniques (different diode absorption lengths, trade-off depending on the current point in the circuit and the insertion losses). No optical switches will be used, which will allow the link latency to be minimized and will lead to deterministic communication times, which are both key features for efficient cache coherence protocols. The second main objective of Opticall^2 is to propose and design a new broadcast-aware cache coherence communication protocol allowing hundreds of computing clusters and memories to be interconnected, which is well adapted to the broadcast-enabled optical communication links. We expect better performance for the parallel execution of benchmark programs, and lower overall power consumption, specifically that due to invalidation or update messages.

7.2.4. ANR SHNOC

Participants: Cédric Killian, Daniel Chillet, Olivier Sentieys, Emmanuel Casseau.

Program: ANR JCJC (young researcher)

Project acronym: SHNOC

Project title: Scalable Hybrid Network-on-Chip

Duration: Feb. 2019 - Jan. 2022

P.I.: C. Killian, CAIRN

The goal of the SHNoC project is to tackle one of the manycore interconnect issues (scalability in terms of energy consumption and latency provided by the communication medium) by mixing emerging technologies. Technology evolution has allowed for the integration of silicon photonics and wireless on-chip communications, creating Optical and Wireless NoCs (ONoCs and WNoCs, respectively) paradigms. The recent publications highlight advantages and drawbacks for each technology: WNoCs are efficient for broadcast, ONoCs have low latency and high integrated density (throughput/cm^2) but are inefficient in multicast, while ENoCs are still the most efficient solution for small/average NoC size. The first contribution of this project is to study the compatibility of processes to associate the three aforementioned technologies and to define an hybrid

topology of the interconnection architecture. This exploration will determine the number of antennas for the WNoC, the amount of embedded lasers sources for the ONoC and the routers architecture for the ENoC. The second main contribution is to provide quality of service of communication by determining, at run-time, the best path among the three NoCs with respect to a target, e.g. minimizing the latency or energy. We expect to demonstrate that the three technologies are more efficient when jointly used and combined, with respect to traffic characteristics between cores and quality of service targeted.

7.2.5. IPL ZEP

Participants: Davide Pala, Olivier Sentieys.

Program: Inria Project Lab

Project acronym: ZEP

Project title: Zero-Power Computing Systems

Duration: Oct. 2017 - Nov. 2020

Coordinator: Inria Socrate

Other partners: Pacap, Cairn, Corse, CEA-LETI

The ZEP project addresses the issue of designing tiny, batteryless, computing objects harvesting energy in the environment. The main application target is Internet of Things (IoT) where small communicating objects will be composed of this computing part associated to a low-power wake-up radio system. The energy level harvested being very low, very frequent energy shortages are expected, which makes the systems following the paradigm of Intermittently-Powered Systems. In order for the system to maintain a consistent state, it will be based on a new architecture embedding non-volatile memory (NVRAM). The major outcomes of the project will be a prototype harvesting board including NVRAM and the design of a new non-volatile processor (NVP) associated with its optimizing compiler and operating system. Cairn is focusing on the microarchitecture of the NVP and on new strategies for backup and restore data and processor state. The ZEP project gathers four Inria teams that have a scientific background in architecture, compilation, operating system and low power together with the CEA Grenoble. Another important goal of the project is to structure the research and innovation that should occur within Inria to prepare the important technological shift brought by NVRAM technologies.

7.2.6. DGA RAPID - FLODAM (2017–2021)

Participants: Joseph Paturel, Simon Rokicki, Olivier Sentieys, Angeliki Kritikakou.

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

7.3. European Initiatives

7.3.1. H2020 ARGO

Participants: Steven Derrien, Angeliki Kritikakou, Olivier Sentieys.

Program: H2020-ICT-04-2015

Project acronym: ARGO

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

Duration: Feb. 2016 - Feb. 2019

Coordinator: KIT

Other partners: KIT (Germany), UR1/Inria/CAIRN, Recore Systems (Netherlands), TEI-WG (Greece), Scilab Ent. (France), Absint (Ger.), DLR (Ger.), Fraunhofer (Ger.)

Increasing performance and reducing cost, while maintaining safety levels and programmability are the key demands for embedded and cyber-physical systems, e.g. aerospace, automation, and automotive. For many applications, the necessary performance with low energy consumption can only be provided by customized computing platforms based on heterogeneous many-core architectures. However, their parallel programming with time-critical embedded applications suffers from a complex toolchain and programming process. ARGO will address this challenge with a holistic approach for programming heterogeneous multi- and many-core architectures using automatic parallelization of model-based real-time applications. ARGO will enhance WCET-aware automatic parallelization by a cross-layer programming approach combining automatic tool-based and user-guided parallelization to reduce the need for expertise in programming parallel heterogeneous architectures. The ARGO approach will be assessed and demonstrated by prototyping comprehensive time-critical applications from both aerospace and industrial automation domains on customized heterogeneous many-core platforms.

7.3.2. ANR International ARTEFaCT

Participants: Olivier Sentieys, Van-Phu Ha, Tomofumi Yuki.

Program: ANR International France-Switzerland

Project acronym: ARTEFaCT

Project title: AppRoximaTivE Flexible Circuits and Computing for IoT

Duration: Feb. 2016 - Dec. 2019

Coordinator: CEA

Other partners: CEA-LETI, CAIRN, EPFL

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

7.4. International Initiatives

7.4.1. Inria International Labs

EPFL-Inria

Associate Team involved in the International Lab:

7.4.1.1. IoTA

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

International Partner (Institution - Laboratory - Researcher):

Ecole Polytechnique Fédérale de Lausanne (Switzerland) - Prof. Christian Enz

Start year: 2017

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

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

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

7.4.2.1. IntelliVIS

Title: Design Automation for Intelligent Vision Hardware in Cyber Physical Systems

International Partner (Institution - Laboratory - Researcher):

IIT Goa (India) - Prof. Sharad Sinha

Start year: 2019

The proposed collaborative research work is focused on the design and development of artificial intelligence based embedded vision architectures for cyber physical systems (CPS). Embedded vision architectures for cyber physical systems (CPS), sometimes referred to as “Visual IoT”, are challenging to design because of primary constraints of compute resources, energy and power management. Embedded vision nodes in CPS, when designed with the application of Artificial Intelligence principles and algorithms, will turn into intelligent nodes (self-learning devices) capable of performing computation and inference at the node resulting in node-level cognition. This would allow only necessary and relevant post processed data to be sent to a human or a computer-based analyst for further processing and refinement in results. However, design and development of such nodes is non-trivial. Many existing computer vision algorithms, typically ported to embedded platforms, are compute and memory intensive thus limiting the operational time when ported to battery powered devices. In addition, transmission of captured visual data, with minimal processing at the node to extract actionable insights poses increased demands on computational, communication and energy requirements. Visual saliency i.e. extraction of key features or regions of interest in images or videos captured by an embedded vision node and related post processing for inference using AI techniques is an interesting and challenging research direction. The primary reason being

that such an approach is expected to cover a wider range of application specific scenarios than statically determined approaches specific to each scenario involving remote off-loading of compute or scenario specific data on servers. Apart from a general approach to visual saliency in nodes using AI based methods (machine and deep learning methods), another principal goal of the proposed project is also to examine and propose methods that allow rapid deployment of AI techniques in these nodes. Many AI techniques are data driven and for a node to adapt from one environment or application specific scenario to another, rapid deployment of AI techniques over the air (OTA) would be an interesting and challenging research direction.

7.4.3. Inria International Partners

7.4.3.1. DARE

Title: Design space exploration Approaches for Reliable Embedded systems

International Partner (Institution - Laboratory - Researcher):

IMEC (Belgium) - Francky Catthoor, IMEC fellow

Duration: 2017 - 2021

Start year: 2017

This collaborative research focuses on methodologies to design low cost and efficient techniques for safety-critical embedded systems, which require high performance and safety implying both fault tolerance and hard real-time constraints. More precisely, the objective is to develop Design Space Exploration (DSE) methodology applicable to any platform domain to drive the design of adaptive predictable low cost and efficient error detection techniques. Run-time dynamic control mechanisms are proposed to actively optimize system fault tolerance by exploring the trade-offs between predictability, reliability, performance and energy consumption using the information received from the environment and the platform during execution. In contrast to design-time static approaches the dynamism can then be exploited to improve energy consumption and performance.

7.4.3.2. LRS

Title: Loop unRolling Stones: compiling in the polyhedral model

International Partner (Institution - Laboratory - Researcher):

Colorado State University (United States) - Department of Computer Science - Prof. Sanjay Rajopadhye

7.4.3.3. HARAMCOP

Title: Hardware accelerators modeling using constraint-based programming

International Partner (Institution - Laboratory - Researcher):

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

7.4.3.4. DeLeES

Title: Energy-efficient Deep Learning Systems for Low-cost Embedded Systems

International Partner (Institution - Laboratory - Researcher):

University of British Columbia (Vancouver, Canada) - Electrical and Computer Engineering - Prof. Guy Lemieux

Start year: 2018

This collaboration is centered around creation of deep-learning inference systems which are energy efficient and low cost. There are two design approaches: (i) an all-digital low-precision system, and (ii) mixed analog/digital low-precision system.

7.4.3.5. Informal International Partners

Dept. of Electrical and Computer Engineering, Concordia University (Canada), Optical network-on-chip, manycore architectures.

LSSI laboratory, Québec University in Trois-Rivières (Canada), Design of architectures for digital filters and mobile communications.

Department of Electrical and Computer Engineering, University of Patras (Greece), Wireless Sensor Networks, Worst-Case Execution Time, Priority Scheduling.

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

PARC Lab., the University of Auckland (New-Zealand), Fault-tolerant task scheduling onto multi-core.

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

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

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Bernard Goossens, Univ. Perpignan, July 2019.
- Sharad Sinha, IIT Goa, India, July 2019.

7.5.2. Visits to International Teams

7.5.2.1. Sabbatical programme

Steven Derrien visited Colorado State University for a 6 month sabbatical from January to July 2019, where he collaborated with Sanjay Rajopadhye. This collaboration has led to two joint PhD between Université de Rennes 1 and Colorado State University which both started in late 2019.

7.5.2.2. Research Stays Abroad

- Olivier Sentieys visited Colorado State University, Computer Science Department and gave a seminar on Approximate Computing in November 2019.
- P. Dobias (PhD student) spent 5 months in the Parallel and Reconfigurable Lab. of the Electrical and Computer Engineering department, the University of Auckland, New Zealand, from November 2018 until March 2019.

CAMUS Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. ADT SPETABARU-H

Participants: Bérenger Bramas, Vincent Loechner, Paul Cardosi.

Duration: 2019 - 2021

The SPETABARU task-based runtime system is now being developed in CAMUS. This tool is the first runtime system build on the tasks and dependencies paradigm that supports speculative execution. It is at the same time a robust runtime system that could be used for high-performance applications, and the central component to perform research in parallelization, speculation and scheduling.

The SPETABARU-H project started in November 2019 for 2 years aims in improving SPETABARU on several aspects:

- Implement a generic speculative execution model based on the team's research;
- Implement the mechanisms to make SPETABARU supporting GPUs (and heterogeneous computing nodes in general);
- Split the management of the workers and the management of the graph of tasks to allow multiple independent graphs to be used on a single node;
- Use SPETABARU in the Complexes++ application, which is a bio-physic software for protein simulation;
- Maintain and update the code to keep it modern and up to date.

9.1.2. Idex Prim'Eau

Participant: Jens Gustedt [contact].

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

9.2. National Initiatives

9.2.1. ANR AJACS

Participant: Arthur Charguéraud.

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

The goal of the AJACS project is to provide strong security and privacy guarantees on the client side for web application scripts implemented in JavaScript, the most widely used language for the Web. The proposal is to prove correct analyses for JavaScript programs, in particular information flow analyses that guarantee no secret information is leaked to malicious parties. The definition of sub-languages of JavaScript, with certified compilation techniques targeting them, will allow us to derive more precise analyses. Another aspect of the proposal is the design and certification of security and privacy enforcement mechanisms for web applications, including the APIs used to program real-world applications. Arthur Charguéraud focuses on the description of a formal semantics for JavaScript, and the development of tools for interactively executing programs step-by-step according to the formal semantics.

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

9.2.2. ANR Vocal

Participant: Arthur Charguéraud.

The Vocal research project is funded by the programme "Société de l'information et de la communication" of the ANR, from October 2015 until October 2020 https://vocal.lri.fr/.

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

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

9.3. European Initiatives

9.3.1. Collaborations with Major European Organizations

Benjamin Stamm and Muhammad Hassan: Université d'Aix-la-Chapelle RWTH, MATHCCES (Germany). An integral equation formulation of the N-body dielectricspheres problem.

Michael Wilczek and Cristian Lalescu: Max Planck Institute for Dynamics and Self-Organization (Germany). Pseudospectral direct numerical simulations (DNS) of the incompressible Navier-Stokes equations.

Juergen Koefinger: Max Planck Institute of Biophysics, Theoretical Biophysics (Germany). Monte-Carlo simulation for coarse grained protein models.

Pavel Kus: Czech Academy of Sciences, Institute of Mathematics (Tchequia). Direct solver for several matrices at a time.

9.4. International Initiatives

9.4.1. Informal International Partners

The CAMUS team has collaborated with the following entities in 2019:

- Reservoir Labs, New York, NY, USA (See subsection 7.3)
- University of Batna, Algeria (See subsection 7.16)
- Universidad Politécnica de Madrid, Spain (See subsection 7.4)
- Barcelona Supercomputing Center, Barcelona, Spain (See subsection 7.5)

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Internships

Toufik Baroudi is a PhD student under the supervision of Rachid Seghir at the University of Batna (Algeria). He is co-advised by Vincent Loechner, and has been visiting our team as an intern for one year from Nov. 2018 to Nov. 2019, founded by the Algerian *Programme National Exceptionnel (PNE)*. His PhD defense is planned at the beginning of 2020.

Raquel Lazcano is a PhD student under the supervision of Eduardo Juárez Martínez at the University of Madrid. She is also co-advised by Philippe Clauss and has been visiting our team as an intern for three months, from February to April 2019. Her PhD defense is planned at the beginning of 2020.

CASH Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Laure Gonnord's "Jeune Chercheur" ANR, CODAS, has started in January 2018 (42 months).

8.1.2. Scientific Advising

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

8.2. International Initiatives

8.2.1. Informal International Partners

- Laure Gonnord has regular collaborations with Fernando Pereira from UFMG, Brasil (5 publications in total, last in 2017). End of 2019 they have restarted discussions with Gabriel Radanne about proving termination properties of linux kernel BPF programs. These programs must be always terminating, and we hope to be able to prove these properties in a scalable way with the termite analyser.
- In 2018 Laure Gonnord has began a collaboration with Tobias Grösser, from ETH Zurich, and in end of 2019 this collaboration has been extended to involved more people of Verimag (David Monniaux) and CASH, in the contexte of a europeean project proposal around certified polyhedral optimisation.
- In 2019, Laure Gonnord has pursued her collaboration with Sebastien Mosser, who moved from univ Nice to UQAM (Quebec, Canada). This collaboration has led to shared interns and a "inria associate team" proposal late in october 2019, which got accepted in January 2019.
- Ludovic Henrio has regular collaborations with: University of Oslo and University of Bergen in Norway (Cristal C. Din, Einar B. Johnsen, and Silvia Lizeth. Tapia Tarifa, Violet K.I. Pun); Reiner Hähnle (TU Darmstadt), Wolfgang Ahrendt (Chalmers); Kiko Fernandez-Reyes, Dave Clarke, and Tobiaas Wrigstad (Univ Uppsala); Christoph Kessler and Ahmed Rezine (Univ of Linköping).

8.3. International Research Visitors

8.3.1. Visits of International Scientists

8.3.1.1. Internships

- Amaury Maillé, M2: from Dec 2018 to Aug 2019 (6 months in total), "Dataflow explicit futures: Formalisation and/or experimentation".
- Julien Rudeau, INSA 4A, from to Apr 2019 to Aug 2019, "Ordonnancement sous contrainte de pipeline", supervised by Christophe Alias.
- Julien Philippon, EPITECH 1A, from to Jul 2019 to Dec 2019, "Compiling dataflow models to circuits", supervised by Christophe Alias and Matthieu Moy.
- Mohamed Hadjoudj, ENS Paris-Saclay 1A, from Jun 2019 to Jul 2019, "Parallélisation sous contrainte de ressources", supervised by Christophe Alias.
- Julian Bruyat, Lyon 1 M1, part-time from January 2019 to May 2019, "Outillage pour l'étude de l'impact de l'ordre des passes de LLVM", supervised by Laure Gonnord and Matthieu Moy.
- Sebastien Michelland, ENS de Lyon M1, abroad co-supervision by Laure Gonnord and Matthieu Moy with main supervision Sebastien Mosser at UQAM (Canada), from May 2019 to July 2019 "Exploration et cartographie des passes de LLVM".

CORSE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. HEAVEN Persyval Project

- Title: HEterogenous Architectures: Versatile Exploitation and programmiNg
- HEAVEN leaders: François Broquedis, Olivier Muller [TIMA lab]
- CORSE participants: François Broquedis, Frédéric Desprez, Georgios Christodoulis, Manuel Selva
- Duration: September 2015 - December 2019
- Abstract: The main objective of this project was to improve the accessibility of heterogeneous architectures comprising FPGA accelerators with portability and real experimentation in mind. The portability criterion allows application programmers to benefit from FPGA devices with only small modifications to their applications. It was achieved by extending a standard parallel programming environment already targeting heterogeneous architectures comprising CPUs and GPUs. During the project, we developed an operational prototype targeting Xilinx FPGAs. Experiments have been conducted using both matrix multiplication and Cholesky decomposition kernels. These experiments have shown the usability of the framework and its very low overhead. This framework opens the path for challenging questions regarding the scheduling of heterogeneous applications targeting FPGAs.

8.2. National Initiatives

8.2.1. IPL ZEP

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

8.3. International Initiatives

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

8.3.1.1. IOComplexity

Title: Automatic characterization of data movement complexity

International Partner (Institution - Laboratory - Researcher):

Ohio State University (United States). P. Sadayappan

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

Start year: 2018

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

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

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

8.4. International Research Visitors

8.4.1. Visits to International Teams

8.4.1.1. Research Stays Abroad

- Fabrice Rastello visited the University of Utah to work with P. Sadayappan during the month of November. He worked on abstract simulation, and optimization of pattern specific programs.
- Nicolas Derumigny visited the University of Utah to work with P. Sadayappan during the month of November. He worked on abstract simulation.
- Nicolas Tollenaere visited the University of Utah to work with P. Sadayappan during the month of November. He worked on abstract simulation, and optimization of convolutions
- Theo Barollet visited the Colorado State University to work with Steve Kommrusch during the month of October. He worked on graph neural networks.
- Nicolas Tollenaere visited the university of Utah to work with P. Sadayappan during the month of August. He worked on optimizing packing and transposition of tensors.

PACAP Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

The Brittany Region is partially funding the PhD fellowship for Niloofar Charmchi on the topic "Hardware prefetching and related issues" and Nicolas Bellec on the topic "Security in real-time embedded systems".

9.2. National Initiatives

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

Participants: Erven Rohou, Bahram Yarahmadi.

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

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

The ZEP project gathers four Inria teams that have a scientific background in architecture, compilation, operating systems together with the CEA Lialp and Lisan laboratories of CEA LETI & LIST [39]. The main application target is Internet of Things (IoT).

9.2.2. NOPE

Participants: Piéric Giraud, Erven Rohou, Bahram Yarahmadi.

NOPE is a one-year exploratory action funded by the Labex Cominlabs. This project aimed at being a first step, and served to elaborate more ambitious future works. Through this project, the consortium was able to grow its knowledge on a topical research theme and lay the foundations of an innovative hardware-software approach. The short term goals were:

- building and sharing across the consortium a strong expertise in state-of-the art results and tools on transient computing, and identifying challenges that should be focused on;
- initiating collaborations between the participants in order to identify opportunities at the hardware-software interface;
- building the foundations of a shared experimental platform for transient computing.

An intern, Piéric Giraud, was hired thanks to NOPE. He ported our WCET infrastructure Heptane to the MSP430 instruction set.

The NOPE project gathers teams PACAP, IETR Syscom and LS2N STR.

9.2.3. Hybrid SIMD architectures (2018–2019)

Participants: Caroline Collange, Alexandre Kouyoumdjian, Erven Rohou.

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

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

9.2.4. DGA/PEC ARMOUR (2018–2021)

Participants: Kévin Le Bon, Erven Rohou.

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

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

9.2.5. ANR DYVE (31/03/2020 – 30/09/2023)

Participants: Arthur Blanleuil, Caroline Collange, Pierre-Yves Peneau.

Most of today's computer systems have CPU cores and GPU cores on the same chip. Though both are general-purpose, CPUs and GPUs still have fundamentally different software stacks and programming models, starting from the instruction set architecture. Indeed, GPUs rely on static vectorization of parallel applications, which demands vector instruction sets instead of CPU scalar instruction sets. In the DYVE project, we advocate a disruptive change in both CPU and GPU architecture by introducing Dynamic Vectorization at the hardware level.

Dynamic Vectorization will combine the efficiency of GPUs with the programmability and compatibility of CPUs by bringing them together into heterogeneous general-purpose multicores. It will enable processor architectures of the next decades to provide (1) high performance on sequential program sections thanks to latency-optimized cores, (2) energy-efficiency on parallel sections thanks to throughput-optimized cores, (3) programmability, binary compatibility and portability.

DYVE is funded by the ANR through the JCJC funding instrument.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ARGO

Participants: Damien Hardy, Isabelle Puaut, Stefanos Skalistis.

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

Program: H2020

Type: RIA

Duration: Jan 2016 – Mar 2019

Coordinator: Karlsruhe Institut für Technologie (Germany)

Université de Rennes 1 contact: Steven Derrien

Partners:

Karlsruher Institut für Technologie (Germany)

SCILAB enterprises SAS (France)

Université de Rennes 1 (France)

Technologiko Ekpaideftiko Idryma (TEI) Dytikis Elladas (Greece)

Absint GmbH (Germany)

Deutsches Zentrum für Luft- und Raumfahrt EV (Germany)

Fraunhofer (Germany)

Increasing performance and reducing costs, while maintaining safety levels and programmability are the key demands for embedded and cyber-physical systems in European domains, e.g. aerospace, automation, and automotive. For many applications, the necessary performance with low energy consumption can only be provided by customized computing platforms based on heterogeneous many-core architectures. However, their parallel programming with time-critical embedded applications suffers from a complex toolchain and programming process. Argo (WCET-Aware PaRallelization of Model-Based Applications for HeteroGeneOus Parallel Systems) will address this challenge with a holistic approach for programming heterogeneous multi- and many-core architectures using automatic parallelization of model-based real-time applications. Argo will enhance WCET-aware automatic parallelization by a crosslayer programming approach combining automatic tool-based and user-guided parallelization to reduce the need for expertise in programming parallel heterogeneous architectures. The Argo approach will be assessed and demonstrated by prototyping comprehensive time-critical applications from both aerospace and industrial automation domains on customized heterogeneous many-core platforms.

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

9.3.1.2. HiPEAC4 NoE

Participants: Pierre Michaud, Erven Rohou, André Seznec, Isabelle Puaut.

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

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

9.3.1.3. Eurolab-4-HPC

Participant: Erven Rohou.

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

Program: H2020

Duration: September 2018 – September 2020

Coordinator: Chalmers Tekniska Hoegskola AB (Sweden)

Partners:

Barcelona Supercomputing Center - Centro Nacional de Supercomputacion (Spain)

Chalmers Tekniska Hoegskola (Sweden)

Foundation for Research and Technology Hellas (Greece)

Universität Stuttgart (Germany)

The University of Manchester (United Kingdom)

Inria (France)

Universität Augsburg (Germany)

ETH Zürich (Switzerland)

École Polytechnique Federale de Lausanne (Switzerland)

Technion - Israel Institute of Technology (Israel)

The University of Edinburgh (United Kingdom)

Rheinisch-Westfaelische Technische Hochschule Aachen (Germany)

Universiteit Gent (Belgium)

Inria contact: Albert Cohen (Inria Paris)

Europe has built momentum in becoming a leader in large parts of the HPC ecosystem. It has brought together technical and business stakeholders from application developers via system software to exascale systems. Despite such gains, excellence in high performance computing systems is often fragmented and opportunities for synergy missed. To compete internationally, Europe must bring together the best research groups to tackle the long-term challenges for HPC. These typically cut across layers, e.g., performance, energy efficiency and dependability, so excellence in research must target all the layers in the system stack. The EuroLab-4-HPC project's bold overall goal is to build connected and sustainable leadership in high-performance computing systems by bringing together the different and leading performance oriented communities in Europe, working across all layers of the system stack and, at the same time, fueling new industries in HPC.

9.4. International Initiatives

9.4.1. ANR CHIST-ERA SECODE 2016–2019

Participants: Damien Hardy, Erven Rohou.

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

CHIST-ERA - RTCPS

Duration: January 2016 – December 2019 (one year extension)

Coordinator: Télécom Paris Tech (France)

Partners:

Télécom Paris Tech (France)

Inria (France)

Université Paris 8 (France)

Sabancı Üniversitesi (Turkey)

Université Catholique de Louvain (Belgium)

Inria contact: Erven Rohou

In this project, we specify and design error correction codes suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects. Such codes mitigate passive attacks, like memory disclosure, and active attacks, like stack smashing. The innovation of this project is to leverage these codes for protecting against both cyber and physical attacks. The main advantage is a full coverage of attacks of the connected embedded systems, which is considered as a smart connected device and also a physical device. The outcome of the project is first a method to generate and execute cyber-resilient software, and second to protect data and its manipulation from physical threats like side-channel attacks.

9.4.2. Informal International Partners

Caroline Collange has collaborated with Marcos Yukio Siraichi, Vinicius Fernandes dos Santos and Fernando Magno Quintão Pereira from UFMG, Brazil [31].

Isabelle Puaut has collaborated with Renato Mancuso (University of Boston, USA) and Heechul Yun (University of Kansas, USA) on predictable memory hierarchies [26]. She has collaborated with Martin Schoeberl (Technical University of Denmark) on predictable branch predictors [29].

Erven Rohou has been collaborating with Prof. Ahmed El-Mahdy (Egypt-Japan University of Science and Technology, Alexandria, Egypt) and his group [21], [22].

Erven Rohou and Loïc Besnard have been collaborating with Prof. João Cardoso (University of Porto, Porto, Portugal) and his group [16].

HYCOMES Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Participants: Benoît Caillaud, Aurélien Lamercerie.

The Hycomes has been participating to the SUNSET project (2016–2019) of the CominLabs excellence laboratory [0]. This project focuses on the computation of surgical procedural knowledge models from recordings of individual procedures, and their execution [28]. The objective is to develop an enabling technology for procedural knowledge based computer assistance of surgery. In this project, we demonstrate its potential added value in nurse and surgeon training. The main contribution of the Hycomes team to this project has been the development of Demodocos, a process model synthesis tool, capable of generating models of a surgical procedure, from a few recordings of actual procedures. Demodocos has been interfaced to the `#SEVEN` virtual reality scenario modeling language and engine, developed in the Hybrid team at Inria Rennes. In 2019, the team has contributed to two publications presenting experimental results of the SUNSET project [9][6].

8.2. National Initiatives

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

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

Name	*Team*	*Inria Center or Laboratory*
Vincent Acary Bernard Brogliato Alexandre Rocca	Tripop	Inria Grenoble Rhône Alpes
Albert Benveniste Benoît Caillaud Khalil Ghorbal Christelle Kozaily Mathias Malandain Benoît Vernay	Hycomes	Inria Rennes Bretagne Atlantique
Marc Pouzet Tim Bourke Imsail Lakhim-Bennani	Parkas	ENS & Inria Paris
Goran Frehse	SSH	ENSTA Paris-Tech.
Antoine Girard		L2S-CNRS, Saclay
Eric Goubault Sylvie Putot	Cosynus	LIX, École Polytechnique, Saclay

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

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

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

In 2019, three general meetings have been organized, with presentations of the partners on new results related to hybrid systems modeling and verification.

Two PhDs are funded by the ModeliScale IPL. Both started in October 2018:

- Christelle Kozaily has started a PhD, under the supervision of Vincent Acary (TRIPOP team at Inria Grenoble), Benoît Caillaud, Khalil Ghorbal on the structural and numerical analysis of non-smooth DAE systems. She is located in the Hycomes team at Inria Rennes.
- Ismail Lahkim-Bennani has started a PhD under the supervision of Goran Frehse (ENSTA Paris-Tech.) and Marc Pouzet (PARKAS team, Inria/ENS Paris). His PhD topic is on random testing of hybrid systems, using techniques inspired by QuickCheck [36].

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

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

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

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

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

In 2019, the effort has been put on the first objective, and two important milestones have been reached:

- The design of a novel algorithm for the structural analysis of multimode DAE systems. This algorithm is a generalization of the Pryce structural analysis method to the multimode case. The key feature of our method is that it works on implicit representations of the set of modes, and of the varying structure of the multimode DAE. In other words, it does not imply the enumeration of the system's modes. Performing the structural analysis at compile-time brings two decisive advantages: 1/ it allows to deliver to the user precise diagnostics about the model, and can be compared type-checking in programming languages; 2/ it is instrumental for the generation of efficient simulation code. Our algorithm is the first method enabling the compile-time analysis of systems with extremely large combinatorics of modes.
- Our multimode DAE structural analysis algorithm has been implemented in IsamDAE, a software comprizing an algorithmic library, to be used in modeling language compilers (Modelica tools) and a standalone tool, to be used independently of a complex Modelica toolset. IsamDAE has allowed to benchmark the method against several families of models, inspired by case-studies developed by industrial partners of the FUI ModeliScale project. Despite the tool is still under development, we have already been able to deal with models with up to 10^{23} modes.

On top of these two main results, the Hycomes team has started investigating the use of Quantized Space Systems (QSS), for the simulation of large DAE systems. QSSs simulation (QSS) was introduced in the early 2000's by F. Cellier and E. Kofman as an alternative to time-based simulation, which is the dominant approach to ODE/DAE systems simulation. Rather than linking QSS to Discrete Event Simulation, we propose to relate it to Synchronous Programming and its continuous time extension Zelus. In the deliverable [20], we expose our understanding of QSS and its variants, then we propose ideas toward a QSS-based cosimulation, by building on top of our knowledge on distributed executions of synchronous programs.

The plan for 2020 is to extend our structural analysis to cover impulsive mode changes and the consistent initialization problem, in the multimode case. A coupling of IsamDAE with Dymola (Dassault Système's commercial implementation of the Modelica language) is under development.

Another future development is to turn our structural analysis method to a compositional method, where large models could be considered by parts. This is a key problem in the Modelica language, as the compilation of a Modelica model is not modular.

Work on QSS methods will continue, and we envision to prototype a QSS-based distributed simulation method for hybrid ODE systems, based on the Zélus language.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

We have a long standing informal collaboration with Martin Otter (DLR, Munich, Germany) and Hilding Helmqvist (Mogram AB, Lund, Sweden). In 2019, this fruitful collaboration has resulted in one publication [7]. The publication draws links between two radically different, but equivalent approaches to the same problem: the impulsive behavior of some multimode DAE, when it is switching from one mode to another. The first approach relies on a transformation of the multimode DAE system to a special index one form, for which state-jumps are proved to be solution of a system of algebraic equations relating right limits to left limits. The second approach builds on the use of nonstandard analysis, combined with the heritage of synchronous programming languages, particularly on the concept of constructive semantics. This gives a formulation of the state-jumps, as a system of difference equations, with an infinitesimal time-step. The latter approach is more general than the former, in the sense that impulsive behavior can be characterized for a larger class of multimode DAE systems. Yet, both approaches coincide on a restricted class of multimode DAEs.

Kairos Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Université Côte d'Azur Academy 1 and EUR DS4H

In the context of the local UCA-Jedi IDEX program and its RISE Academy, we were afforded a three years funding, including a postdoctoral position, for the "Smart IoT for Mobility" project. This project, lead by the LEAT UMR and Kairos, aims at building a formal language for the design of smart contracts in the context of a mobility project, in collaboration with Renault Software Labs and Symag, a subsidiary of BNP Paribas. This agreement was operational in preparing the larger ANR project SIM, that was accepted this year, while an even larger European project is under proposal.

9.1.2. PSPC-Region project ADAVEC

This project was recently accepted, and not yet started in practice. It associates Renault Software Labs with UCA (represented by our team), together with Avisto Telecom and EPICnPOC companies. The focus is on requirements and specification for Automated Driving Assistance, and more specially the transitions that need to be properly handled when control needs to be held back to the human driver.

9.2. National Initiatives

9.2.1. ANR Project SIM

The ANR SIM (Smart IoT for Mobility) is a PRCE project co-funded by ANR (AAPG 2019) and DGA for 42 months. The national coordinator is the LEAT (UMR CNRS) and the other partners are Renault Software Labs and Symag. The goal is to provide a formal meta-language to describe smart contracts that can be used in the context of an autonomous vehicles to provide services to the users. The services are related to the combined use of multi-model transportation systems by having a single smart contracts that can enforce all the intermediate transactions with all the actors involved (car manufacturing, parking lease, highway toll companies, insurances, bike rental companies).

9.2.2. Competitivity Clusters

The Kairos team is involved in the actions of the cluster SCS (Systèmes Communicants Sécurisés) and Frédéric MALLET is elected in the steering committee of SCS. One of the more prominent action is to build, in partnership with University Aix-Marseille, a Digital Innovation Hub, to open the access (with actions of transfer and valorization) to Digital Innovations for companies that would benefit from it, like public institutions (hospitals, human resources, employment institutions) or private companies that could use IoT for agriculture, tourism, smart infrastructures (harbours, buildings, cities).

9.2.3. CNRS GDRs

We are registered members of three GDR funded by CNRS : **SoC**^{2}, on topics of Hardware-software codesign and Non-Functional Property modeling for co-simulation; **LTP**, on verification and language design for reactive CPS systems; **GPL**, on software engineering and Domain-Specific Languages.

9.2.4. Inria Project Lab SPAI

This collaborative action, targeting *Security by Program Analysis for the IoT (SPAI)*, is headed by the Indes Project, and associated the Antique, Privatics and Celtique EPIs. See 7.15 for our contribution.

9.2.5. PAI ES3CAP

ES3CAP (Embedded Smart Safe Secure Computing Autonomous Platform) is a PIA (Programme d'Investissements d'Avenir) project. Its budget is of 22.2MEuros, over 36 months. The national coordinator is Kalray, and other partners include Safran, Renault, and MBDA. The objectives of the 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 will 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.

Our technical contributions to this project are described in 7.16 . This project partially finances Hugo Pompugnac's PhD and Jad Khatib's post-doc.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. IIP TuMuLT

Title: Trustworthy Modeling using Logical Time

International Partner (Institution - Laboratory - Researcher):

E.C.N.U. (Shanghai, China) - Departement of Software Engineering and Computer Science - Zhang Min

Duration: 2018 - 2022

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

- Modeling the Uncertain Environments of Cyber-Physical Systems: Logical Time is one of the main scientific foundation of the KAIROS Team. From the background in theory of concurrency, we are used to consider mainly discrete control systems that can guarantee a functional determinism independently of any implementation-specific timing variation. Addressing Cyber-Physical Systems and the Internet of Things means widening those assumptions to consider the external environment, typically involving uncertainty, as part of the design. This task explores the definition of sound extensions to logical time to capture both the physical continuous behavior and make an abstract characterization as a statistical approximation.
- SMT For Logical Time: While synchronous systems usually focus on finite state-based control systems, our abstraction of logical time relies on both Boolean algebra (for synchronous operations) and integer arithmetic (for synchronizing mechanisms), In that context, SMT is a promising solution to solve systems that combine several theories. We had first results on this aspect [SCP'17] but we still need to increase the subset of constraints that can be addressed efficiently as well as the performances of the solving tools.
- Spatio-Temporal Specification for Trustworthy Intelligent Transportation Systems: Focusing on Intelligent Transportation Systems as a subset of Cyber-Physical Systems, we encounter specific problems. This task would focus on extensions of our framework for a spatio-temporal logics based on logical time. This means a description of the location of infrastructures as well as the ability to build constraints that depend both on time (logic or physical) and locations (logical or physical).

- Symbolic approaches for models and analysis of Open systems: Methods for analyzing and guaranteeing the properties of critical and complex systems, including their data and time depend aspects, have strongly evolved with the emergence of efficient SAT and SMT engines. We are working on novel methods combining classical verification paradigms with SMT approaches to create symbolic and compositional verification methods and tool platforms [22], [27].

  Collaboration will come in the form of scientific short or middle term visits, student exchanges (master and PhD), and organization of events (workshops and conferences).

9.3.1.2. Informal International Partners

- Luigi Liquori has a steady collaboration with researchers from University of Udine and Turin, Italy.
- We keep close informal relations with the Universities of Kiel and Bamberg Germany, in the context of the Synchronous Reactive academic community. We all attended the yearly Synchron seminar, held this year in Aussois (together with researchers from Verimag and the Parkas and Spades Inria teams).
- Frédéric Mallet has a collaboration with Peter Olvecsky from University of Oslo. He was funded in 2019 by a program of the French Embassy in Norway called Asgard.

9.3.2. Participation in Other International Programs

- PHC Cai Yuan Pei: The partnership is a joint funding from Campus France and Chinese Scholarship Council (CSC) to fund short exchanges of permanent staffs and long exchanges of PhD students. A 2-week visit was carried out by Frédéric Mallet in 2019, while Xiaohong Chen is visiting France during 3 months starting in mid-November. The program is funded for three years and a PhD student (Zhang Juan) will visit our team during 16 months in 2020.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Xiaohong Chen, Assistant Professor at East China Normal University (Shanghai), from Nov 2019 to Feb 2020.
- Grygoriy Zholtkevych, Professor at V.N. Karazin Kharkiv National University (Ukraine), from Oct 2019 until Nov 2019.
- Peter Olvescky, Professor at University of Oslo, from November 24th to November 29th, 2019.
- Matteo Sereno, Professor, University of Turin, Italy, in May 2019.
- Thomas Ehrhard, University of Paris, in September 2019.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

- E. Madelaine spent 4 weeks visiting the Software Engineering an Computer Science department at ECNU Shanghai (2 weeks in May, 2 weeks in September), founded by the foreign expert program of ECNU; and 1 week visiting the Institute of Software of the Chinese Academy of Science (ISCAS, Beijing), funded by ISCAS.
- Marie-Agnès Peraldi Frati spent 10 days at Danang University in May 2019 in the context of the joined UCA/UD international DNIIT laboratory for student supervision and scientific meetings. The visit was funded by Mobility Contract Erasmus Mundus.
- Frédéric Mallet stayed three weeks in Shanghai in August 2019. He stayed one week in Hangzhou in September as part of a Chinese competition for oversea professors. He also stayed two weeks in Shanghai in November 2019 through the PHC Cai Yuan Pei program.

KOPERNIC Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FUI

8.1.1.1. CEOS

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

8.2. European Initiatives

8.2.1. Collaborations with Major European Organizations

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

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

8.3. International Research Visitors

8.3.1. Visits of International Scientists

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

8.3.1.1. Internships

- Kartikeya Singh (India).

PARKAS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

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

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

This project continues.

8.1.2. FUI: Fonds unique interministériel

8.1.2.1. Modeliscale contract (AAP-24)

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

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

8.1.3.1. ES3CAP collaborative project (Bpifrance)

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

8.1.4. Others

8.1.4.1. Inria Project Lab (IPL) Modeliscale

This project treats the modelling and analysis of Cyber-Physical Systems at large scale. The PARKAS team contributes their expertise in programming language design for reactive and hybrid systems to this multi-team effort.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

- MNEMOSENE is a project with funding from the European Union's Horizon 2020 Research and Innovation Programme. Its objectives include the improvement of the energy-delay product, the computational efficiency and performance density by several orders of magnitude compared to state-of-the-art architectures. A cornerstone of the proposed solution is the memristor-based Compute-in-Memory (CIM) architecture, which eliminates long-distance, high-latency data transfers between memory and computing units required in conventional Von Neumann-based architectures by carrying out computations for performance-critical operations directly in memory.
- TETRAMAX, *Technology Transfer via Multinational Application Experiments*, is funded by the H2020 "Smart Anything Everywhere (SAE)" initiative. The overall ambition is to build and leverage a European Competence Center Network in customized low-energy computing, providing easy access for SMEs and mid-caps to novel CLEC technologies via local contact points. This is a bidirectional interaction: SMEs can demand CLEC technologies and solutions via the network, and vice versa academic research institutions can actively and effectively offer their new technologies to European industries. Furthermore, TETRAMAX wants to support 50+ industry clients and 3rd parties with innovative technologies, using different kinds of Technology Transfer Experiments (TTX) to accelerate innovation within European industries and to create a competitive advantage in the global economy.

8.3. International Initiatives

8.3.1. Participation in Other International Programs

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

SPADES Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. CASERM (Persyval-Lab project)

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

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

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

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

The CASERM consortium gathers researchers from the LIG and VERIMAG laboratories who are reknowned specialists in these fields. The project started in November 2016 and was completed in November 2019.

8.1.2. SEC: Construction of Safe Explainable Cyber-physical systems

Participants: Gregor Goessler, Thomas Mari.

In cyber-physical systems (CPS), software interacts with physical processes so as achieve desired functionalities. CPS are usually subject to safety and reliability requirements. Depending on the application, their failure may have unacceptable consequences, it is therefore crucial to ensure their correctness at design time. In addition, explainability of increasingly autonomous CPS is becoming crucial in order for the CPS to be socially acceptable.

The goal of this project is twofold. First, we will investigate a contract-based design approach for safe CPS in which different aspects – such as functional requirements, real-time constraints, and continuous behaviors – are modeled and verified separately. Second, we will leverage the contracts in order to ensure explainability of the system behavior by construction. By explainability we understand, informally, that for any behavior of the system we can automatically construct, from a log generated by the execution, an excerpt that retains only the events that causally contributed to the outcome, and that is easy to understand by a human expert.

The SEC project is supported by the "Initiatives de Recherche Stratégiques (IRS)" program of the IDEX UGA. It funds the PhD thesis of Thomas Mari, who will be co-advised by Gregor Gössler and Thao Dang (VERIMAG).

8.2. National Initiatives

8.2.1. ANR

8.2.1.1. RT-proofs

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

RT-proofs is an ANR/DFG project between Inria, MPI-SWS, Onera, TU Braunschweig and Verimag, running from 2018 until 2022.

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

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

The results obtained in 2019 in connection with the RT-proofs project are described in Section 6.2.4 .

8.2.1.2. DCore

Participants: Gregor Goessler, Jean-Bernard Stefani.

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

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

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

8.2.2. Institute of Technology (IRT)

8.2.2.1. CAPHCA

Participants: Alain Girault, Nicolas Hili.

CAPHCA is a project within the Antoine de Saint Exupéry IRT in Toulouse. The general objective of the project is to provide methods and tools to achieve both performance and determinism on modern, high-performance, multi-core and FPGA-enabled SOCs. Our specific contribution lies withing work packages dedicated to the design of novel PRET architectures and programming languages (see Section 6.2.1). This contract has yielded two publications so far [17], [16].

8.3. European Initiatives

8.3.1. Collaborations in European Programs, Except FP7 & H2020

Program: Celtic-Plus

Project acronym: SENDATE

Project title: Secure Networking for a Data center cloud in Europe

Duration: April 2016 - March 2019

Coordinator: Nokia France

Other partners: Nokia, Orange, IMT, Inria

Abstract: The SENDATE project aims to develop a clean-slate architecture for converged telecommunications networks and distributed data centers supporting 5G cellular networks and the needs from the Industrial Internet and the Internet of Things. It aims to provide scientific and technical solutions for intra and inter data centrers security, control, management and orchestration, placement and management of virtual network functions, as well as high-speed transport networks for data centers access and interconnection.

8.3.2. Collaborations with Major European Organizations

We have a strong collaboration with the Technische Universität Braunschweig in Germany and the MPI-SWS in Kaiserslautern (Germany) on formal proofs for the analysis real-time systems. This collaboration is formalized by the ANR-PRCI project called RT-proofs started in 2018, which involves MPI-SWS, TU Braunschweig, Inria, and Onera.

8.4. International Initiatives

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

8.4.1.1. Quasar

Title: Quantitative systems formal verification

International Partner (Institution - Laboratory - Researcher):

CAS (China) - Department of Informatics - Lijun Zhang

Start year: 2019

The general scientific objectives are to extend formal analysis and verification methods such as model checking, process algebra and interactive theorem proving (Coq) to quantitative systems, more specifically probabilistic and quantum computing systems. Application fields include compositional modeling for dynamic real-time probabilistic software architectures and risk analysis. The collaboration will involve active scientists on all these fields not only from Inria and Inst Soft. CAS, but also from CWI, Verimag Grenoble, ECNU Shanghai, and partners of CWI (VU Amsterdam and Twente).

TEA Project-Team

9. Partnerships and Cooperations

9.1. International Initiatives

9.1.1. Inria International Labs

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

9.1.1.1. CONVEX

Title: Compositional Verification of Cyber-Physical Systems

International Partner (Institution - Laboratory - Researcher):

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

Start year: 2018

See also: http://convex.irisa.fr

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

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

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

Inria@SiliconValley
Associate Team involved in the International Lab:

9.1.1.2. Composite

Title: Compositional System Integration

International Partners (Institution - Laboratory - Researcher):

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

Start year: 2017

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

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

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

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

9.1.1.3. Inria International Chairs

IIC GUPTA Rajesh

Title: End-to-end system co-design

International Partner (Institution - Laboratory - Researcher):

University of California, San Diego (United States) - Rajesh Gupta

Duration: 2017 - 2021

Start year: 2017

9.1.1.4. Insa-Inria International Chair

Shuvra Bhattacharyya

Title: System design methodologies for real-time signal and information processing

International Partner (Institution - Laboratory - Researcher):

University of Maryland (United States) - Shuvra Bhattacharyya

Duration: 2018 - 2021

Start year: 2017

9.2. International Research Visitors

9.2.1. Visits of International Scientists

- Shuvra Bhattacharyya (UMD) visited project-team TEA and IETR in the context of his Insa-Inria Chair in May, July and December. He gave numerous talks and organized a workshop for the preparation of a European project proposal.
- Rajesh Gupta (UCSD) visited project-team TEA in the context of his Inria Chair in July and gave a seminar entitled: programming human spaces.
- Niki Vazou (IMDEA) visited project-team TEA in May and gave a presentation on her POPL'20 paper: "Liquidate your assets: reasoning about resource usage in Liquid Haskell".
- Yamine Ait Ameur (IRIT) visited project-team TEA in January on the occasion of Simon Lunel's Thesis defense.
- Naijun Zhan (ISCAS) visited project-team TEA in July, in the context of associate-project CONVEX.

- Delegates of the Sheng Yuan Honors College (BUAA) visited Inria-Irisa and Ecole Normale Supérieur de Rennes for the prospect of initiating an exchange program for graduate students, which will start in 2020.
- Zhang Bojun and Wang Zikai (BUAA) visited project-team TEA in July for an internship on verified modeling of blockchain protocols in Coq.
- Shenghao Yuan (NUAA) visited project-team TEA in July, in the context of associate-team CONVEX, and gave a presentation of the verified mini-Signal code generator developed at Nanhang University.

9.2.2. Visits to International Teams

Jean-Pierre Talpin visited UC San Diego in March, in the context of the associate-team Composite, and visited ISCAS, Beijing, in May and October, in the context of the associate-team CONVEX.

ANTIQUE Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. AnaStaSec

Title: Static Analysis for Security Properties

Type: ANR générique 2014

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2015 - September 2019

Coordinator: Inria Paris-Rocquencourt (France)

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

Inria contact: Jérôme Feret

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

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

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

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

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

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

9.1.2. DCore

Title: DCore - Causal Debugging for Concurrent Systems

Type: ANR générique 2018

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: March 2019 - February 2023

Coordinator: Inria Grenoble - Rhône-Alpes (France)

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

Inria contact: Jérôme Feret

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

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

The overall objective of the project is to develop a semantically well-founded, novel form of concurrent debugging, which we call "causal debugging", that aims to alleviate the deficiencies of current debugging techniques for large concurrent software systems.

Briefly, the causal debugging technology developed by the DCore project will comprise and integrate two main novel engines:

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

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

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

9.1.3. REPAS

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

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

9.1.4. SAFTA

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

Type: ANR JCJC 2018

Duration: February 2018 - August 2022

Coordinator: Cezara Drăgoi, CR Inria

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

9.1.5. TGFSYSBIO

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

Type: Plan Cancer 2014-2019

Duration: December 2015 - September 2019

Coordinator: INSERM U1085-IRSET

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

Inria contact: Jérôme Feret

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

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

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

9.1.6. VeriAMOS

Title: Verification of Abstract Machines for Operating Systems

Type: ANR générique 2018

Defi: Société de l'information et de la communication

Instrument: ANR grant

Duration: January 2019 - December 2022

Coordinator: Inria Paris (France)

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

Inria contact: Xavier Rival

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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Type: IDEAS

Defi:

Instrument: ERC Proof of Concept Grant 2018

Objectif: Static Analysis for the VErification of Spreadsheets

Duration: January 2019 - June 2020

Coordinator: Inria (France)

Partner: None

Inria contact: Xavier Rival

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

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

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

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

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

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

9.4. International Research Visitors

9.4.1. Visits of International Scientists

9.4.1.1. Internships

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

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

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

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

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

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

CAMBIUM Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR projects

8.1.1.1. Vocal

Participants: Armaël Guéneau, Xavier Leroy, François Pottier.

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

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

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

8.2. International Research Visitors

8.2.1. Visits of International Scientists

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

CELTIQUE Project-Team

5. Partnerships and Cooperations

5.1. National Initiatives

5.1.1. The ANR Scrypt project

Participants: Frédéric Besson, Sandrine Blazy, Thomas Jensen, David Pichardie, Alexandre Dang, Remi Hutin.

Security, Secure compilation

The Scrypt project (ANR-18-CE25-0014) aims at providing secure implementations of crypto-graphic primitives using formal methods and secure compilation techniques. One specific goal is to design secure compilers which preserve the security of the source code against side-channel attacks.

This is a joint project with the Inria team MARELLE, École Polytechnique and AMOSSYS.

5.1.2. The ANR MALTHY project

Participant: David Cachera.

The MALTHY project, funded by ANR in the program INS 2013, aims at advancing the state-of-the-art in real-time and hybrid model checking by applying advanced methods and tools from linear algebra and algebraic geometry. MALTHY is coordinated by VERIMAG, involving CEA-LIST, Inria Rennes (Tamis and Celtique), Inria Saclay (MAXPLUS) and VISEO/Object Direct.

5.1.3. The ANR AJACS project

Participants: Thomas Jensen, Alan Schmitt.

The goal of the AJACS project is to provide strong security and privacy guarantees on the client side for web application scripts. To this end, we propose to define a mechanized semantics of the full JavaScript language, the most widely used language for the Web. We then propose to develop and prove correct analyses for JavaScript programs, in particular information flow analyses that guarantee no secret information is leaked to malicious parties. The definition of sub-languages of JavaScript, with certified compilation techniques targeting them, will allow us to derive more precise analyses. Finally, we propose to design and certify security and privacy enforcement mechanisms for web applications, including the APIs used to program real-world applications.

The project partners include the following Inria teams: Celtique, Indes, Prosecco, and Toccata; it also involves researchers from Imperial College as external collaborators. The project runs from December 2014 to March 2019.

5.1.4. The ANR DISCOVER project

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

The DISCOVER project project (2014–09/2019) aims at leveraging recent foundational work on formal verification and proof assistants to design, implement and verify compilation techniques used for high-level concurrent and managed programming languages. The ultimate goal of DISCOVER is to devise new formalisms and proof techniques able to scale to the mechanized correctness proof of a compiler involving a rich class of optimizations, leading to efficient and scalable applications, written in higher-level languages than those currently handled by cutting-edge verified compilers.

In the light of recent work in optimizations techniques used in production compilers of high-level languages, control-flow-graph based intermediate representations seems too rigid. Indeed, the analyses and optimizations in these compilers work on more abstract representations, where programs are represented with data and control dependencies. The most representative representation is the sea-of-nodes form, used in the Java Hotspot Server Compiler, and which is the rationale behind the highly relaxed definition of the Java memory model. DISCOVER proposes to tackle the problem of verified compilation for shared-memory concurrency with a resolute language-based approach, and to investigate the formalization of adequate program intermediate representations and associated correctness proof techniques.

The project started in October 2014 and ended on September 2019.

5.1.5. The ANR CISC project

Participants: Frédéric Besson, Thomas Jensen, Alan Schmitt.

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

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

5.2. European Initiatives

5.2.1. FP7 & H2020 Projects

5.2.1.1. The ERC VESTA project

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

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

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

5.2.1.2. The SPARTA cybersecurity competence network

Participants: Thomas Jensen, Frédéric Besson.

SPARTA is a novel Cybersecurity Competence Network, supported by the EU's H2020 program, with the objective to develop and implement top-tier research and innovation collaborative actions. Guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA will set up unique collaboration means, leading the way in building transformative capabilities and forming a world-leading Cybersecurity Competence Network across the EU. The SPARTA consortium assembles 44 actors from 14 EU Member States at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity.

Celtique is coordinating the Inria participation in the SPARTA network. The team contributes to the programme on intelligent infrastructures with techniques for building security-enhanced systems code that respects strong information flow constraints. The team is also leading the elaboration of the SPARTA scientific roadmap, in collaboration with TU Munich.

5.2.2. Collaborations in European Programs, Except FP7 & H2020

Program:CA COST Action CA15123

Project acronym: EUTYPES

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

Duration: 03/2016 to 03/2020

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

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

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

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

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

5.3. International Initiatives

5.3.1. WEBCERT

Title: Verified Trustworthy web Applications

International Partner (Institution - Laboratory - Researcher):

Imperial College London - Department of Computing - Philippa Gardner

Duration: 2015 - 2019

Start year: 2015

See also: JSCert web page

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

CONVECS Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. ARC6 Programme

Participants: Lina Marsso, Radu Mateescu [correspondent], Wendelin Serwe.

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

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

9.2. National Initiatives

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

9.2.1.1. CAPHCA

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

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

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

9.2.2. Competitivity Clusters

9.2.2.1. SECURIOT-2

Participants: Hubert Garavel [correspondent], Armen Inants, Radu Mateescu, Wendelin Serwe.

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

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

9.2.3. Other National Collaborations

We had sustained scientific relations with the following researchers:

- Xavier Etchevers (Orange Labs, Meylan),
- Fabrice Kordon and Lom Messan Hillah (LIP6, Paris),
- Eric Jenn and Viet Anh Nguyen (IRT Saint-Exupéry, Toulouse),
- Michel Le Pallec (Nokia Bell Labs, Nozay),
- Chu-Min Li (University of Picardie Jules Verne),
- Ioannis Parissis and Oum-El-Kheir Aktouf (LCIS, Valence),
- Pascal Poizat (LIP6, Paris).

9.3. European Initiatives

9.3.1. Collaborations with Major European Organizations

The CONVECS project-team is member of the FMICS (*Formal Methods for Industrial Critical Systems*) working group of ERCIM [0]. H. Garavel and R. Mateescu are members of the FMICS board, H. Garavel being in charge of dissemination actions.

9.4. International Initiatives

H. Garavel is a member of IFIP (*International Federation for Information Processing*) Technical Committee 1 (*Foundations of Computer Science*) Working Group 1.8 on Concurrency Theory chaired successively by Luca Aceto and Jos Baeten.

9.4.1. Inria International Partners

9.4.1.1. Informal International Partners

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

9.4.2. Other International Collaborations

In 2019, we had scientific relations with several universities and institutes abroad, including:

- University of Málaga, Spain (Francisco Durán),
- University of Cali, Colombia (Camilo Rocha),
- University of Zaragoza, Spain (José Ignacio Requeno),
- ISTI/CNR, Pisa, Italy (Franco Mazzanti),
- FBK, Trento, Italy (Enrico Magnano),
- Aalto University, Finland and Northeastern University, Boston, Massachusetts (Stavros Tripakis),
- Saarland University, Germany (Holger Hermanns),
- Eindhoven University of Technology, The Netherlands (Anton Wijs and Sander de Putter),
- University of Zielona Gora, Poland (Remigiusz Wisniewski).

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

9.5. International Research Visitors

9.5.1. Visits of International Scientists

- H. Garavel is an invited professor at Saarland University (Germany) as a holder of the Gay-Lussac Humboldt Prize.
- Hernan Ponce de Leon (Fortiss, Munich, Germany) visited us on June 25–26, 2019. He gave a lecture entitled "*BMC with Weak Memory Models*".
- Hugues Evrard (Google, London, UK) visited us on October 21, 2019. He gave a lecture entitled "*GPU Schedulers: How Fair is Fair Enough?*".
- Karoliina Lehtinen (University of Liverpool, UK) visited us on October 23, 2019. She gave a lecture entitled "*Quasi-Polynomial Techniques for Parity Games and Other Problems*".
- Peter Csaba Ölveczky (University of Oslo, Norway) visited us on November 25, 2019. He gave a lecture entitled "*Formal Specification and Analysis of Real-Time Systems in Real-Time Maude*".

The annual CONVECS seminar was held in Villard-de-Lans (France) on July 1-3, 2019. The following invited scientists attended the seminar:

- Loïc Letondeur (Orange Labs) gave on July 2, 2019 a talk entitled "*Artificial Intelligence and Edge Computing*".
- Eric Jenn (IRT Saint-Exupéry / Thales Avionics) gave on July 3, 2019 a talk entitled "*Recent Achievements of the CAPHCA Project*".
- Viet Anh Nguyen (IRT Saint-Exupéry) gave on July 3, 2019 a talk entitled "*Using Model Checking to Identify Timing Interferences on Multicore Processors*".

DEDUCTEAM Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

Valentin Blot obtained funding for hiring Étienne Miquey as a post-doctoral researcher from Île-de-France region's DIM-RFSI (Domaine d'Intérêt Majeur - Réseau Francilien en Sciences Informatiques).

8.2. National Initiatives

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

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

Frédéric Blanqui cooperates with various researchers in Japan: Makato Hamana (Gunma University), Yoji Akama (Tohoku University) and Kentaro Kikuchi (Tohoku University).

8.4. International Research Visitors

8.4.1. Visits to International Teams

8.4.1.1. Research Stays Abroad

Gilles Dowek has spent two weeks at the Institute of Software in Beijing where he has worked with Ying Jiang, Wu Peng, and Wenhui Zhang.

Gilles Dowek has spent two weeks at the University of Buenos Aires where he has worked with Alejandro Díaz-Caro.

Frédéric Blanqui has been invited for two weeks in Japan by Yoji Akama (Tohoku University) and Makato Hamana (Gunma University).

As a "Short Term Scientific Mission" financed by COST Action EUTypes, Guillaume Genestier spent five weeks in Chalmers University, Gothenburg, Sweden, to cooperate with Jesper Cockx and Andreas Abel on the translation between the proof assistant Agda and Dedukti.

GALLINETTE Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

Vercoma (Atlanstic 2020/Attractivity grant)

Goal: Verified computer mathematics.

Coordinator: A. Mahboubi.

Duration: 08/2018 - 08/2021.

7.2. National Initiatives

7.2.1. ANR

FastRelax (ANR-14-CE25-0018).

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

Coordinator: Bruno Salvy (Inria, ENS Lyon).

Participant: A. Mahboubi.

Duration: 2014-2019.

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

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

7.3. European Initiatives

7.3.1. FP7 & H2020 Projects

7.3.1.1. CoqHoTT

Title: Coq for Homotopy Type Theory

Programm: H2020

Type: ERC

Duration: June 2015 - May 2020

Coordinator: Inria

Inria contact: Nicolas TABAREAU

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

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

Program: COST

Project acronym: EUTYPES

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

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

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

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

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

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

7.4. International Initiatives

7.4.1. Inria International Labs

Inria Chile

Associate Team involved in the International Lab:

7.4.1.1. GECO

Title: Gradual verification and robust proof Engineering for COq

International Partner (Institution - Laboratory - Researcher):

Universidad de Chile (Chile) - Centrum Wiskunde & Informatica - Éric Tanter

Start year: 2018

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

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

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

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

7.4.2. Inria International Partners

7.4.2.1. Informal International Partners

- A. Mahboubi holds a part-time endowed professor position in the Department of Mathematics at the Vrije Universiteit Amsterdam (the Netherlands).

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Matias Toro (U. Chile) visited 1 week in January to work with G. Munch-Maccagnoni.

7.5.2. Visits to International Teams

7.5.2.1. Research Stays Abroad

+ G. Munch-Maccagnoni visited E. Tanter and M. Toro (U. Chile) in March.

MEXICO Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- MATTHIAS FUEGGER is co-leading the Digicosme working group *HicDiesMeus* on *Highly Constrained Discrete Agents for Modeling Natural Systems*.
- STEFAN HAAR is co-leading the Digicosme working group *TheoBioR* on *Computational methods for modelling and analysing biological networks*.

8.2. National Initiatives

- Thomas Chatain, Stefan Haar, Serge Haddad and Stefan Schwoon are participating in the ANR Project ALGORECELL.
- Matthias Függer participates in the ANR project FREDDA on verification and synthesis of distributed algorithms.

8.3. International Research Visitors

8.3.1. Visits of International Scientists

- Susanna DONATELLI was invited professor of ENS Paris-Saclay during one month in January, working with Serge Haddad on the expressiveness and conciseness of temporal logic for Markov chains. This work was also coninued durin a visit of Serge Haddad at the university of Torino in March. Their joint work has led to a publication to appear in the international conference LATA 2020 at Milano.
- Sven DZIADEK, Sep-Nov 2019 (PhD student, Univ. Leipzig)

8.3.1.1. Research Stays Abroad

- JURAJ KOLCˇÁK visited the SDM group of Hasuo Ichiro at NII Tokyo from August 2018 to February 2019, working in particular on differential logics.

MOCQUA Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- Project acronym: ANR PRCE SoftQPro (ANR-17-CE25-0009)
  Project title: Solutions logicielles pour l'optimisation des programmes et ressources quantiques.
  Duration: Dec. 2017 - Dec. 2022
  Coordinator: Simon Perdrix
  Other partners: Atos-Bull, LRI, CEA-Saclay.
  Participants: Simon Perdrix, Emmanuel Jeandel, Emmanuel Hainry, and Romain Péchoux
  Abstract: Quantum computers can theoretically solve problems out of reach of classical computers. We aim at easing the crucial back and forth interactions between the theoretical approach to quantum computing and the technological efforts made to implement the quantum computer. Our software-based quantum program and resource optimisation (SoftQPRO) project consists in developing high level techniques based on static analysis, certification, transformations of quantum graphical languages, and optimisation techniques to obtain a compilation suite for quantum programming languages. We will target various computational model back-ends (e.g. QRAM, measurement-based quantum computations) as well as classical simulation. Classical simulation is central in the development of the quantum computer, on both ends: as a way to test quantum programs but also as a way to test quantum computer prototypes. For this reason we aim at designing sophisticated simulation techniques on classical high-performance computers (HPC).
- Project acronym: ANR PRCI VanQuTe (ANR-17-CE24-0035)
  Project title: Validation of near-future quantum technologies.
  Duration: Fev. 2018 - Jan. 2022
  Coordinator: Damian Markham (Laboratoire d'informatique de Paris 6)
  Other partners: NTU (Nanyang Technological University), SUTD (Singapore University of Technology and Design), NUS (Nationl University of Singapore), LIP6 (Laboratoire d'informatique de Paris 6)
  Participants: Simon Perdrix, Emmanuel Jeandel
  Abstract: In the last few years we have seen unprecedented advances in quantum information technologies. Already quantum key distribution systems are available commercially. In the near future we will see waves of new quantum devices, offering unparalleled benefits for security, communication, computation and sensing. A key question to the success of this technology is their verification and validation.

  Quantum technologies encounter an acute verification and validation problem: On one hand, since classical computations cannot scale-up to the computational power of quantum mechanics, verifying the correctness of a quantum-mediated computation is challenging. On the other hand, the underlying quantum structure resists classical certification analysis. Members of our consortium have shown, as a proof-of-principle, that one can bootstrap a small quantum device to test a larger one. The aim of VanQuTe is to adapt our generic techniques to the specific applications and constraints of photonic systems being developed within our consortium. Our ultimate goal is to develop techniques to unambiguously verify the presence of a quantum advantage in near future quantum technologies.

8.1.2. Other initiatives

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

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Mathieu Hoyrup participates in the Marie-Curie RISE project Computing with Infinite Data coordinated by Dieter Spreen (Univ. Siegen) that has started in April 2017.

8.3. International Initiatives

8.3.1. Participation in Other International Programs

ECOS-Sud A17C03 QuCa - 01/2018 - 12/2020. **Quantum Calculi**. Funded by MinCyT and ECOS France.
Argentine Director: A. Díaz-Caro (UNQ/CONICET), French Director: G. Dowek (Inria, LSV, ENS Paris-Saclay)
Permanent members: P. Arrighi (Aix-Marseille) - J.-Y. Marion (LORIA) - P. E. Martínez López (UNQ) - S. Perdrix - B. Valiron (CentraleSupélec).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Alonso Herrera: Universidad Andrés Bello, Chile.
- Takayuki Kihara : Nagoya University, Japan.
- Damiano Mazza, CNRS, LIPN.
- Victor Selivanov: Ershov Institute of Informatics Systems, Novosibirsk, Russia.

8.4.2. Visits to International Teams

8.4.2.1. Research Stays Abroad

Simon Perdrix visited Universita Buenos Aires, Universita de Quilmes and Conicet for two weeks in November 2019. The visit was part of the QuCa Ecos Sud project and was partially funded by LIA SINFIN.

PARSIFAL Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. DIM-RFSI

Gabriel Scherer obtained funding from the Région Île-de-France to hire a post-doc, Luc Pellissier, to work on canonical representation of programs (linking proof theory and category-theory approaches), in collaboration with Adrien Guatto in IRIF (Université Paris 7).

9.2. National Initiatives

9.2.1. ANR

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

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

9.2.2. Competitivity Clusters

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

9.3. International Research Visitors

9.3.1. Visits of International Scientists

Claudio Sacerdoti Coen (Universita di Bologna, Italy) spent a month visiting Beniamino Accattoli thanks to funding for short-term international visits.

PI.R2 Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

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

Pierre-Louis Curien, Yves Guiraud (local coordinator until Sept. 2019) and Matthieu Sozeau are members of the GDR Topologie Algébrique, federating French researchers working on classical topics of algebraic topology and homological algebra, such as homotopy theory, group homology, K-theory, deformation theory, and on more recent interactions of topology with other themes, such as higher categories and theoretical computer science.

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

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

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

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

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

Yann Régis-Gianas collaborates with Nomadic Labs on the topic of certified smart contract compilation.

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

Yann Régis-Gianas and Alexis Saurin (coordinator) are members of the four-year RAPIDO ANR project, started in January 2015 and ended in September 2019. RAPIDO aims at investigating the use of proof-theoretical methods to reason and program on infinite data objects. The goal of the project is to develop logical systems capturing infinite proofs (proof systems with least and greatest fixpoints as well as infinitary proof systems), to design and to study programming languages for manipulating infinite data such as streams both from a syntactical and semantical point of view. Moreover, the ambition of the project is to apply the fundamental results obtained from the proof-theoretical investigations (i) to the development of software tools dedicated to the reasoning about programs computing on infinite data, *e.g.* stream programs (more generally coinductive programs), and (ii) to the study of properties of automata on infinite words and trees from a proof-theoretical perspective with an eye towards model-checking problems. Other permanent members of the project are Christine Tasson from IRIF (PPS team), David Baelde from LSV, ENS-Cachan, and Pierre Clairambault, Damien Pous and Colin Riba from LIP, ENS-Lyon.

Matthieu Sozeau is a member of the CoqHoTT project led by Nicolas Tabareau (Gallinette team, Inria Nantes & École des Mines de Nantes), funded by an ERC Starting Grant, ending in 2020. The PhD grant of Antoine Allioux is funded by the CoqHoTT ERC.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, Except FP7 & H2020

- Program: COST
- Project acronym: EUTypes
- Project title: The European research network on types for programming and verification
- Duration: March 2016 - March 2020
- Coordinator: Herman Geuvers
- Other partners: 29 countries
- Abstract: This COST promotes (1) the synergy between theoretical computer scientists, logicians and mathematicians to develop new foundations for type theory (2) the joint development of type theoretic tools as proof assistants and integrated programming environments, (3) the study of dependent types for programming and its deployment in software development, (4) the study of dependent types for verification and its deployment in software analysis and verification.

8.3. International Initiatives

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

Pierre-Louis Curien and Claudia Faggian are members of the CRECOGI associate team, coordinated on one side by Ugo dal Lago (research-team FoCUS, Inria Sophia and Bologna), and on the other side by Ichiro Hasuo (NII, Tokyo). The full name of the project is Concurrent, Resourceful and full Computation, by Geometry of Interaction. This project was renewed in 2019 for a duration of two years.

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

8.3.2. Inria International Partners

8.3.2.1. Participation in International Programs

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

8.3.2.2. International Initiatives

Pierre-Louis Curien is principal investigator on the French side for a joint project Inria - Chinese Academy of Sciences. The project's title is "Verification, Interaction, and Proofs" (December 2017 – December 2020). The principal investigator on the Chinese side is Ying Jiang, from the Institute of Software (ISCAS) in Beijing. The participants of the project on the French side are Pierre-Louis Curien and Jean-Jacques Lévy, as well as other members of IRIF (Thomas Ehrhard, Jean Krivine, Giovanni Bernardi, Ahmed Bouajjani, Mihaela Sighireanu, Constantin Enea, Gustavo Petri), and Gilles Dowek (Deducteam team of Inria Saclay). On the Chinese side, the participants are Ying Jiang, as well as other members of the ISCAS (Angsheng Li, Xinxin Liu, Yi Lü, Peng Wu, Yan Rongjie, Zhilin Wu, and Wenhui Zhang), and Yuxi Fu (from Shanghai Jiaotong University).

8.4. International Research Visitors

8.4.1. Research Stays Abroad

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

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

STAMP Project-Team

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR

- FastRelax, "Fast and Reliable Approximations", started on October 1st, 2014, for 60 months (ending in September 2019), with a grant of 75 kEuros for Marelle. Other partners are Inria Grenoble (ARIC project-team), LAAS-CNRS (Toulouse), Inria Saclay (Toccata and Specfun project-teams), and LIP6-CNRS (Paris). The corresponding researcher for this contract is Laurence Rideau.
- TECAP "Analyse de protocoles, Unir les outils existants", starting on October 1st, 2017, for 60 months, with a grant of 89 kEuros. Other partners are Inria teams PESTO (Inria Nancy grand-est), Ecole Polytechnique, ENS Cachan, IRISA Rennes, and CNRS. The corresponding researcher for this contract is Benjamin Grégoire.
- SafeTLS "La sécurisation de l'Internet du futur avec TLS 1.3" started on October 1st, 2016, for 60 months, with a grant of 147kEuros. Other partners are Université de Rennes 1, and secrétariat Général de la Défense et de la Sécurité Nationale. The corresponding researcher for this contract is Benjamin Grégoire.
- BRUTUS "Chiffrements authentifiés et résistants aux attaques par canaux auxiliaires", started on October 1st, 2014, for 60 months, with a grant of 41 kEuros for STAMP. Other partners are Université de Rennes 1, CNRS, secrétariat Général de la défense et de la sécurité nationale, and Université des Sciences et Technologies de Lille 1. The corresponding researcher for this contract is Benjamin Grégoire.
- Scrypt "Compilation sécurisée de primitives cryptographiques" started on February 1st, 2019, for 48 months, with a grant of 100 kEuros. Other partners are Inria team Celtique (Inria Rennes Bretagne Atlantique), Ecole polytechnique, and AMOSSYS SAS. The corresponding researcher for this contract is Benjamin Grégoire.

7.1.2. FUI

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

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

7.2. European Initiatives

7.2.1. Collaborations in European Programs, Except FP7 & H2020

Program: COST

Project acronym: EUTypes

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

Coordinator: Prof. Herman Geuvers, Radboud University, The Netherlands

Abstract: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.

7.2.2. Collaborations with Major European Organizations

Partner 1: MPI Bochum, Gilles Barthe, Germany

Formally verified cryptography

7.3. International Initiatives

7.3.1. Informal International Partners

We have strong collaborations with AIST in Japan. Reynald Affeldt, a researcher from AIST has been visiting our team since October 1st 2019. The topic of choice is formalization of a variety of topics using the Mathematical Components library, aiming mostly at formalizing robotics.

7.4. International Research Visitors

7.4.1. Visits of International Scientists

We received the visit of Marc Gourjon (Technische Universität Hamburg) in April and from Manuel Barbosa (University of Porto) in June and July.

We received the visit of Reynald Affeldt (AIST, Japan) starting on October 1st.

We received the visit of Kazuhiko Sakaguchi (University of Tsukuba), from January 1st to October 31st.

SUMO Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

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

- Individual grant, led by Nicolas Markey

The objective of this project is to explore two research directions in the continuity of recent works: a truly quantitative theory of formal verification on the one hand, and the development of strategy-synthesis algorithms for modular systems on the other hand. It ended in June 2019.

9.2. National Initiatives

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

- Link to website
- Led by Ocan Sankur (SUMO);
- SUMO participants: Emily Clément, Léo Henry, Thierry Jéron, Nicolas Markey, Victor Roussanaly, Ocan Sankur
- Partners: LSV (Cachan), ISIR (Paris), LaBRI (Bordeaux), LRDE (Paris), LIF (Marseille)

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

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

- Link to website
- Led by David Gross-Amblard (Université Rennes 1);
- Participants : Éric Badouel, Loïc Hélouët, Adrian Puerto Aubel, Rituraj Singh;
- Partners: Inria Project-Teams Valda (Paris), DRUID (Rennes), SUMO (Rennes), Links (Lille), MNHN, Foule Factory.

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

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

- Link to website
- Led by Arnaud Legrand (Inria Grenoble Rhône-Alpes)
- Participants: Thierry Jéron, The Anh Pham.
- Partners: Inria project-teams Avalon (Lyon), POLARIS (Grenoble), HiePACS, STORM (Bordeaux), MExICo (Saclay), MYRIADS, SUMO (Rennes), VeriDis (Nancy).

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

This year we have been mainly interested in the extension of the SimGrid programming model of MPI with synchronization primitives, the formalisation in ATL, of this model, and its adaptation to dynamic partial-order-reduction methods (DPOR) that allow to reduce the explored state space. A prototype implementation of an existing method that combines DPOR with true-concurrency models has been experimented on toy examples. The Anh Pham completed his PhD in december 2019.

9.2.4. National informal collaborations

The team collaborates with the following researchers:

- Béatrice Bérard (LIP6, Paris 6) on problems of opacity and diagnosis, and on problems related to logics and partial orders for security;
- Patricia Bouyer (LSV, ENS Paris-Saclay) on the analysis of probabilistic timed systems and quantitative aspects of verification;
- Thomas Chatain and Stefan Haar (Inria team MExICo, LSV, ENS Paris-Saclay) on topics related to concurrency and time, and to modeling and verification of metro networks, multimodal systems and passenger flows;
- Gwenaël Delaval and Éric Rutten (Inria team Ctrl-A, LIG, Université Grenoble-Alpes) on the control of reconfigurable systems and the link between Reax and Heptagon/BZR (http://bzr.inria.fr/);
- Serge Haddad (Inria team MExICo, LSV, ENS Paris-Saclay) on opacity and diagnosis;
- Loïg Jézéquel (LS2N, Université de Nantes) on stochastic and timed nets, and on distributed optimal planning;
- Didier Lime and Olivier H. Roux (LS2N, Université de Nantes) on stochastic and timed Petri nets;
- François Laroussinie (IRIF, UP7-Diderot) on logics for multi-agent systems,

9.3. International Initiatives

9.3.1. Inria International Labs

LIRIMA: International Laboratory for Research in Computer Science and Applied Mathematics

9.3.1.1. FUCHSIA

Associate Team involved in the international lab LIRIMA.

Title: Flexible user-centric higher-order systems for collective intelligence in agencies

International Partner

U. Yaoundé (Cameroon) Georges-Edouard Kouamou

Start year: 2019

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

Develop methods and tools, based on guarded attribute grammars, to design flexible and adaptive systems for information gathering and deliberation in order to collaboratively build expertise in health emergency situations.

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

9.3.2.1. EQUAVE

Title: Efficient Quantitative Verification

International Partner

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

Start year: 2018

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

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

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

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

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

9.3.3. Inria International Partners

9.3.3.1. Informal International Partners

The team collaborates with the following researchers:

- S. Akshay (IIT Bombay, India) on timed concurrent models;
- Andrea D'Ariano (University Roma Tre, Italy), on train regulation.
- Christel Baier (Technical University of Dresden, Germany) on verification and control of stochastic systems;
- Thomas Brihaye (Université de Mons, Belgium) on the verification of stochastic timed systems;
- Gilles Geeraerts and Jean-François Raskin, (Université Libre de Bruxelles, Belgium) on multiplayer game theory and synthesis;
- Alessandro Giua and Michele Pinna (University Cagliari, Italy) on diagnosis and unfolding techniques for concurrent systems.

- Igor Konnov (Interchain, Austria), Marijana Laźic (Technical University Munich, Germany) and Josef Widder (Interchain, Austria) on the automated verification of randomized distributed algorithms.
- Stéfane Lafortune (University of Michigan, USA) on the control of cyber-physical systems;
- Kim G. Larsen (University Aalborg, Denmark) on quantitative timed games, and on topics related to urban train systems modeling;
- John Mullins (Polytechnique Montréal, Canada) on security and opacity;
- Mickael Randour (Université de Mons, Belgium) on quantitative games for synthesis.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- S. Akshay (IIT Bombay, India) visited the team for one week.
- Christel Baier and Jakob Piribauer (TU Dresden, Germany) visited the SUMO team for one week in september.
- Khushraj Nanik Madnani (IIT Bombay, India) visited our team during two months.
- Laurie Ricker (Mount Allison University, Canada) visited the team during 2 months.
- Graeme Zinck (Mount Allison University, Canada) visited our team during four months. He obtained a 5000$ grant provided by Mitacs through a collaboration between Mount Allison University (L. Ricker) and Inria (Loïc Hélouët and Hervé Marchand). Two papers are in preparation (one regarding the enforcement of opacity for modular systems (submitted to Ifac World congress) and the other about the enforcement of concurrent secrets for multiple systems.

9.4.1.1. Internships

- Pierre Boudart, ENS Ulm, June-July 2019, Éric Fabre.
- Kritin Garg and Sharvik Mital, IIT Bombay, May-July 2019, Éric Fabre, Blaise Genest and Loïc Hélouët.
- Mathieu Poirier, ENS Rennes, May-July 2019, Éric Badouel and Adrian Puerto Aubel.
- Bastien Thomas, ENS Rennes, Feb-July 2019, Nathalie Bertrand.

TOCCATA Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. ELEFFAN

Participant: Sylvie Boldo [contact].

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

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

Partners: ENSTA Paristech (A. Chapoutot)

9.1.2. MILC

Participant: Sylvie Boldo [contact].

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

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

9.2. National Initiatives

9.2.1. ANR CoLiS

Participants: Claude Marché [contact], Andrei Paskevich.

The CoLiS research project is funded by the programme "Société de l'information et de la communication" of the ANR, for a period of 60 months, starting on October 1st, 2015. http://colis.irif.univ-paris-diderot.fr/

The project aims at developing formal analysis and verification techniques and tools for scripts. These scripts are written in the POSIX or bash shell language. Our objective is to produce, at the end of the project, formal methods and tools allowing to analyze, test, and validate scripts. For this, the project will develop techniques and tools based on deductive verification and tree transducers stemming from the domain of XML documents.

Partners: Université Paris-Diderot, IRIF laboratory (formerly PPS & LIAFA), coordinator; Inria Lille, team LINKS

9.2.2. ANR Vocal

Participants: Jean-Christophe Filliâtre [contact], Andrei Paskevich.

The Vocal research project is funded by the programme "Société de l'information et de la communication" of the ANR, for a period of 60 months, starting on October 1st, 2015. See https://vocal.lri.fr/

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

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

9.2.3. FUI LCHIP

Participant: Sylvain Conchon [contact].

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

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

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

9.2.4. ANR PARDI

Participant: Sylvain Conchon [contact].

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

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

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. EMC2

Participant: Sylvie Boldo [contact].

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

9.3.2. Collaborations in European Programs, Except FP7 & H2020

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

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

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

Duration: 2015-2019

Coordinator: Herman Geuvers, Radboud University Nijmegen, The Netherlands

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

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

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

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Jorge Sousa Pinto, professor from Universidade do Minho (Braga, Portugal, https://haslab.uminho.pt/jsp/) visited the team for 1 month in May 2019. We interact with him on the topic of the formalization of VC generation algorithms [21]. He also proposed a formalization using the Why3 tool.

VERIDIS Project-Team

9. Partnerships and Cooperations

9.1. Regional Initiatives

Antoine Defourné's PhD thesis and Yann Duplouy's post-doctoral research are co-funded by Région Grand Est.

9.2. National Initiatives

9.2.1. PIA2 ISITE LUE

Project acronym: ISITE LUE - Digitrust

Project title: Lorraine Université d'Excellence, Citizen Trust in the Digital World

Duration: 2016 – 2020

Coordinator: Marine Minier

Participants: Margaux Durœulx, Stephan Merz

Abstract: Digitrust is one of the "impact" projects within the excellence funding acquired by University of Lorraine and supports research into different aspects related to the trustworthiness and security of digital systems. It funds the PhD thesis of Margaux Durœulx on the use of SAT techniques for assessing system reliability.

9.2.2. ANR International Project ProMiS

Project acronym: ProMiS.

Project title: Provable Mitigation of Side Channel through Parametric Verification

Duration: November 2019 – April 2022.

Coordinators: Étienne André and Jun Sun (Singapore Management University, Singapore).

Other partners: École Centrale Nantes, Singapore University of Technology and Design.

Participants: Étienne André.

Abstract: ProMiS is an international project, funded by ANR in France and by NRF in Singapore under the PRCI program.

The Spectre vulnerability has recently been reported, which affects most modern processors. The idea is that attackers can extract information about the private data using a timing attack. It is an example of side channel attacks, where secure information flows through side channels unintentionally. How to systematically mitigate such attacks is an important and yet challenging research problem.

We propose to automatically synthesize mitigation of side channel attacks (e.g., timing or cache) using well-developed verification techniques. The idea is to reduce this problem to the parameter synthesis problem of a given formalism (for instance, parametric timed automata). Given a program or system with design parameters which can be tuned to mitigate side channel attacks, our approach will automatically generate provably secure valuations of the parameters. We plan to deliver a toolkit which can be automatically applied to real-world systems.

9.2.3. ANR International Project SYMBIONT

Project acronym: SYMBIONT.

Project title: Symbolic Methods for Biological Networks.

Duration: July 2018 – June 2021.

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

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

Participants: Thomas Sturm, Hamid Rahkooy.

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

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

9.2.4. ANR Project Formedicis

Project acronym: Formedicis.

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

Duration: January 2017 – December 2020.

Coordinator: Bruno d'Augsbourg (Onera).

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

Participants: Dominique Méry, Horatiu Cirstea.

Abstract: During the last 30 years, the aerospace domain has successfully devised rigorous methods and tools for the development of safe functionally-correct software. During this process, interactive software has received a relatively lower amount of attention. However, Human-System Interactions (HSI) are important for critical systems and especially in aeronautics: for example, the investigation into the crash of the Rio-Paris flight AF 447 in 2009 pointed out a design issue in the Flight Director interface as one of the original causes of the crash. Formedicis aims at designing a formal hub language, in which designers can express their requirements concerning the interactive behavior that must be embedded inside applications, and at developing a framework for validating, verifying, and implementing critical interactive applications expressed in that language.

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

9.2.5. ANR Project DISCONT

Project acronym: DISCONT.

Project title: Correct integration of discrete and continuous models.

Duration: March 2018 – February 2022.

Coordinator: Paul Gibson (Telecom Sud Paris), until February 2019; Dominique Méry, since March 2019.

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

Participants: Dominique Méry, Zheng Cheng.

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

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

9.2.6. ANR Project PARDI

Project acronym: PARDI.

Project title: Verification of parameterized distributed systems.

Duration: January 2017 – December 2021.

Coordinator: Philippe Quéinnec (ENSEEIHT/IRIT Toulouse).

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

Participants: Igor Konnov, Stephan Merz.

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

More information: http://pardi.enseeiht.fr/.

9.2.7. Inria IPL HAC SPECIS

Project acronym: HAC SPECIS.

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

Duration: June 2016 – June 2020.

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

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

Participants: Marie Duflot-Kremer, Stephan Merz.

Abstract: The goal of HAC SPECIS is to allow the study of real HPC systems with respect to both correctness and performance. To this end, this Inria Project Lab assembles experts from the HPC, formal verification, and performance evaluation communities. VeriDis contributes its expertise in formal verification techniques. In particular, our goal is to extend the functionalities of exhaustive and statistical model checking within the SimGrid platform. Yann Duplouy joined the project in December 2018 as a post-doctoral researcher with the objective of designing and implementing a statistical model checker for SimGrid.

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

9.2.8. DFG Transregional Research Center 248 CPEC

Project acronym: CPEC.

Project title: Foundations of Perspicuous Software Systems.

Duration: January 2019 – December 2022.

Coordinators: Holger Hermanns (Saarland University, Germany) and Raimund Dachselt (University of Dresden, Germany).

Other partners: Max Planck Institute for Software Systems, Saarbrücken.

Participants: Alberto Fiori, Sophie Tourret, Christoph Weidenbach.

Abstract: With cyber-physical technology increasingly impacting our lives, it is very important to ensure that humans can understand them. Systems lack support for making their behaviour plausible to their users. And even for technology experts it is nowadays virtually impossible to provide scientifically well-founded answers to questions about the exact reasons that lead to a particular decision, or about the responsibility for a malfunctioning. The root cause of the problem is that contemporary systems do not have any built-in concepts to explicate their behaviour. They calculate and propagate outcomes of computations, but are not designed to provide explanations. They are not perspicuous. The key to enable comprehension in a cyber-physical world is a science of perspicuous computing.

More information: https://www.perspicuous-computing.science/.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

9.3.1.1. ERC Matryoshka

Program: ERC.

Project acronym: Matryoshka.

Duration: April 2017 – March 2022.

Coordinator: Jasmin Blanchette (VU Amsterdam).

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

Abstract: Proof assistants are increasingly used to verify hardware and software and to formalize mathematics. However, despite some success stories, they remain very laborious to use. The situation has improved with the integration of first-order automatic theorem provers – superposition provers and SMT (satisfiability modulo theories) solvers – but only so much can be done when viewing automatic provers as black boxes. The purpose of Matryoshka is to deliver much higher levels of automation to users of proof assistants by fusing and extending two lines of research: automatic and interactive theorem proving. Our approach is to enrich superposition and SMT with higher-order (HO) reasoning in a careful manner, in order to preserve their desirable properties. With higher-order superposition and higher-order SMT in place, we will develop highly automatic provers building on modern superposition provers and SMT solvers, following a novel stratified architecture, and integrate them in proof assistants. Users stand to experience substantial productivity gains: From 2010 to 2016, the success rate of automatic provers on interactive proof obligations from a representative benchmark suite called Judgment Day has risen from 47% to 77%; with this project, we aim at 90%–95% proof automation.

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

9.3.2. Collaborations in European Programs, Except FP7 & H2020

Program: Erasmus+.

Project acronym: PIAF.

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

Coordinator: Université de Liège.

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

Participant: Marie Duflot-Kremer.

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

Program: ERASMUS+.

Project acronym: ARC.

Project title: Automated reasoning in the class.

Coordinator: West University of Timisoara (Romania).

Other partners: Johaness Kepler University Linz (Austria), RWTH Aachen University (Germany), Eszterhazy Karoly University (Hungary), Université de Lorraine.

Participant: Sorin Stratulat.

Abstract: The main objective of the project is to improve the education of computer science students in fields related to computational logic, by creating innovative and advanced learning material that uses automated reasoning and by training a large number of academic staff in using this in a modern way. Thus indirectly the project objectives include the effects of increased software reliability: virus elimination, online safety, better detection of negative online phenomena (fake news, cyberbullying, etc.), and other.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

Maria Paola Bonacina.

Date: 11 February 2019 – 16 February 2019.

Institution: Università degli Studi di Verona, Italy.

Host: Pascal Fontaine.

Maria Paola Bonacina is a professor at the Università degli Studi di Verona, Italy. She is well known in the community for her numerous works in the field of automated reasoning, notably in SMT, combination of theories, and procedures for first-order logic. During her one-week stay in Nancy, we particularly discussed SGGS (semantically-guided goal-sensitive theorem proving) as a means of inspiration for instantiation in SMT. We also worked on a review paper on combination of theories, published in 2019 [49].

Armin Biere.

Date: 27 May 2019 – 29 May 2019.

Institution: Johannes Keppler Universität, Linz, Austria.

Host: Christoph Weidenbach.

Armin Biere is professor at the University of Linz. He is a leading researcher in the SAT community. During his stay we discussed recent developments in SAT solving. In particular, resolution based inference and reduction mechanisms beyond subsumption resolution.

9.4.1.1. Internships

Manon Blanc

Date: 1 June 2019 – 31 July 2019

Institution: ENS Cachan

Host: Pascal Fontaine

In her bachelor thesis, Manon Blanc studied and experimentally evaluated two different subtropical methods for handling polynomial constraints within SMT.

Mehran Aghabozorgi

Date: 5 August 2019 – 7 October 2019

Institution: Isfahan University of Technology, Iran

Host: Christoph Weidenbach

Mehran worked on algorithms enhancing SAT pre- and inprocessing. He implemented blocked clause elimination as well as a variable elimination algorithm aiming at smaller clause sets.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Thomas Sturm visited the University of Bonn (Institute of Computer Science II) for 4 weeks during 2019, and the University of Kassel (Mathematical Institute). Topics included perspectives for SMT Solving in symbolic reaction network analysis, toricity of steady state varieties, scaling methods for systems of ordinary differential equations (ODE), and logic approaches for the classification of real singularities of ODE.

CIDRE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **Labex COMINLABS contract (2016-2019): "BigClin" - https://bigclin.cominlabs.u-bretagneloire.fr/fr**

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

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

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

8.2. National Initiatives

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

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

8.3. International Research Visitors

8.3.1. Research Stays Abroad

Emmanuelle Anceaume has been invited by the University of La Sapienza (Italy) from the 1st to the 30th of September 2019. During this stay, she collaborated with Profs Leonardo Querzony and Giuseppe A. Di Luna. Their collaboration gave rise to an implementation of the Replicated State Machine, which is resilient to Byzantine behaviors in asynchronous environments [18] (will appear at IPDPS in 2020).

8.4. European Initiatives

8.4.1. H2020 Projects

- **SPARTA (2019-2022) - https://www.sparta.eu/**

  SPARTA is a Cybersecurity Competence Network supported by the EU's H2020 program (Grant agreement ID: 830892) and led by CEA. This 3 years project started in February 2019. It aims to coordinate and develop the implementation of high-level research and innovation in digital security, in order to strengthen the strategic autonomy of the European Union.The CIDRE team is involved both in the workpackage 2 (SPARTA Roadmap) that aims to develop an ambitious Cybersecurity Research and Innovation Roadmap and the workpackage 6 (SPARTA Program HAII-T) that will develop a foundation for secure-by-design Intelligent infrastructures. More precisely, in the context of a task dedicated to resilience-by-design, we design an intrusion detection mechanism that combines both signature-based and anomaly-based approaches.

COMETE Project-Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. LOST2DNN

Program: DATAIA Call for Research Projects

Project title: Leakage of Sensitive Training Data from Deep Neural Networks

Duration: October 2019 - September 2022

Coordinators: Catuscia Palamidessi, Inria Saclay, EPI Comète and Pablo Piantanida, Centrale Supèlec

Other PI's and partner institutions: Georg Pichler, TU Wien, Austria

Abstract: The overall project goal is to develop a fundamental understanding with experimental validation of the information-leakage of training data from deep learning systems. More specifically, we aim at:

- Developing a compelling case study based on state-of-the-art algorithms to perform model inversion attacks, showcasing the feasibility of uncovering specified sensitive information from a trained software (model) on real data.
- Quantifying information leakage. Based on the uncovered attacks, the amount of sensitive information present in trained software will be measured or quantified. The resulting measure of leakage will serve as a basis for the analysis of attacks and for the development of robust mitigation techniques.
- Mitigating information leakage. Strategies will be explored to avoid the uncovered attacks and minimize the potential information leakage of a trained model.

8.2. National Initiatives

8.2.1. REPAS

Program: ANR Blanc

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

Duration: October 2016 - September 2021

Coordinator: Catuscia Palamidessi, Inria Saclay, EPI Comète

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

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

8.3. European Initiatives: FP7 & H2020 Projects

8.3.1. HYPATIA

Program: European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme.

Project acronym: HYPATIA

Project title: Privacy and Utility Allied

Duration: October 2019 – September 2024

Principal Investigator: Catuscia Palamidessi

Abstract: With the ever-increasing use of internet-connected devices, such as computers, smart grids, IoT appliances and GPS-enabled equipments, personal data are collected in larger and larger amounts, and then stored and manipulated for the most diverse purposes. Undeniably, the big-data technology provides enormous benefits to industry, individuals and society, ranging from improving business strategies and boosting quality of service to enhancing scientific progress. On the other hand, however, the collection and manipulation of personal data raises alarming privacy issues. Not only the experts, but also the population at large are becoming increasingly aware of the risks, due to the repeated cases of violations and leaks that keep hitting the headlines.

The objective of this project is to develop the theoretical foundations, methods and tools to protect the privacy of the individuals while letting their data to be collected and used for statistical purposes. We aim in particular at developing mechanisms that can be applied and controlled directly by the user thus avoiding the need of a trusted party, are robust with respect to combination of information from different sources, and provide an optimal trade-off between privacy and utility.

8.4. International Initiatives

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

8.4.1.1. LOGIS

Title: Logical and Formal Methods for Information Security

Inria principal investigator: Konstantinos Chatzikokolakis

International Partners:

Mitsuhiro Okada, Keio University (Japan)

Yusuke Kawamoto, AIST (Japan)

Tachio Terauchi, JAIST (Japan)

Masami Hagiya, University of Tokyo (Japan)

Start year: January 2019 - December 2021.

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

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

8.4.2. Inria International Partners

Geoffrey Smith, Florida International University, USA

Carroll Morgan, NICTA , Australia

Annabelle McIver, Maquarie University, Australia

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

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia

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

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

8.4.3. Participation in Other International Programs

8.4.3.1. CLASSIC

Program: Colciencias - Conv. 712.

Project acronym: CLASSIC.

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

Duration: Oct 2016 - Oct 2019.

URL: http://goo.gl/Gv6Lij

Coordinator: Camilo Rueda, Universidad Javeriana de Cali, Colombia.

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

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

8.4.3.2. FACTS

Program: ECOS NORD.

Project acronym: FACTS.

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

Duration: Jan 1 2019 - Dec 31, 2021.

URL: https://goo.gl/zVhg32

Coordinator: Frank Valencia, Ecole Polytechnique.

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

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

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Yusuke Kawamoto, Researcher, AIST, Japan, AIST, March 2019 and Nov-Dec 2019

Takao Murakami, Researcher, AIST, Japan, AIST, March 2019

Sophia Knight, Assistant Professor, University of Minnesota, USA, May 2019

Carlos Olarte, Assistant Professor, Universidade Federal do Rio Grande do Norte, Brazil. Nov 2019

Camilo Rueda, Professor, Universidad Javeriana de Cali, Colombia. May-July 2019

Mario Ferreira Alvim Junior, Assistant Professor, Federal University of Minas Gerais, Brazil. Nov 2019

Sergio Ramirez, PhD student, Universidad Javeriana de Cali, Colombia. Oct-Dec 2019

Carlos Pinzon, Master student, Universidad Javeriana de Cali, Colombia. Nov 2019

8.5.2. Internships

Sayan Biswas, Master student, Univ. of Bath, UK. From Jun 2019 until Sep 2019

Noemie Fong, Master student, ENS Paris. Jan-Feb 2019

Federica Granese, Univ. Od Rome "La Sapienza", Italy. From Mar 2019 until Jun 2019

Boammani Lompo, ENS Rennes. From May 2019 until Jul 2019

DATASPHERE Team

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

8.2. National Initiatives

- Chaire Castex, Ecole Militaire, Paris.
- AMNECYS (Alpine Multidisciplinary NEtwork on CYber-security Studies), University of Grenoble-Alpes.
- GEODE Research team on Geopolitics.
- Kavé Salamatian in co-leading the chair "AI and society" of the MIAI institute of University of Grenoble Alps.

8.3. International Initiatives

8.3.1. Inria International Partners

8.3.1.1. Informal International Partners

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

8.4. International Research Visitors

8.4.1. Visits to International Teams

8.4.1.1. Research Stays Abroad

Stéphane Grumbach has been visiting scientist at the Research Institute on Humanity and Nature, RIHN, in Kyoto for a semester in 2018/2019.

PESTO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

- ANR SEQUOIA *Security properties, process equivalences and automated verification*, duration: 4 years, since October 2014, leader: Steve Kremer, other partners: ENS Cachan, Univ Luxembourg. Most protocol analysis tools are restricted to analyzing reachability properties while many security properties need to be expressed in terms of some process equivalences. The increasing use of observational equivalence as a modeling tool shows the need for new tools and techniques that are able to analyze such equivalence properties. The aims of this project are *(i)* to investigate which process equivalences — among the plethora of existing ones — are appropriate for a given security property, system assumptions and attacker capabilities; *(ii)* to advance the state of the art of automated verification for process equivalences, allowing for instance support for more cryptographic primitives, relevant for case studies; *(iii)* to study protocols that use low-entropy secrets expressed using process equivalences; *(iv)* to apply these results to case studies from electronic voting.
- ANR TECAP *Protocol Analysis — Combining Existing Tools*, duration: 4 years, starting in 2018, leader: Vincent Cheval, other partners: ENS Cachan, Inria Paris, Inria Sophia Antipolis, IRISA, LIX. Despite the large number of automated verification tools, several cryptographic protocols (e.g. stateful protocols) still represent a real challenge for these tools and reveal their limitations. To cope with these limits, each tool focuses on different classes of protocols depending on the primitives, the security properties, etc. Moreover, the tools cannot interact with each other as they evolve in their own model with specific assumptions. The aim of this project is to get the best of all these tools, that is, to improve the theory and implementations of each individual tool towards the strengths of the others and to build bridges that allow the cooperations of the methods/tools. We will focus in this project on CryptoVerif, EasyCrypt, Scary, ProVerif, *TAMARIN*, *Akiss* and APTE. In order to validate the results obtained in this project, we will apply our results to several case studies such as the Authentication and Key Agreement protocol from the telecommunication networks, the Scytl and Helios voting protocols, and the low entropy 3D-Secure authentication protocol. These protocols have been chosen to cover many challenges that the current tools are facing.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

- SPOOC (2015–2020) [0]— ERC Consolidator Grant on Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols.

  The goals of the Spooc project are to develop solid foundations and practical tools to analyze and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. We will
  - develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties;
  - develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms;
  - apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without the need to trust the voter client software.

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

Steve Kremer is the leader of the project.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

- Collaboration with David Basin, Ralf Sasse and Lara Schmid (ETH Zurich), Cas Cremers (Helmholtz Center for Information Security (CISPA)), and Sasa Radomirovic (Univ Dundee) on the improvement of the *TAMARIN* prover
- Collaboration with David Basin and Lara Schmid (ETH Zurich) on the study of the security impact of the bulletin board in e-voting protocols
- Collaboration with Guillaume Girol (CEA), David Basin, Ralf Sasse (ETH Zurich), Dennis Jackson (Univ Oxford), and Cas Cremers (Helmholtz Center for Information Security (CISPA)) on a new security analysis framework for the Noise language
- Collaboration with Ravishankar Borgaonkar (Sintef), Shinjo Park, and Altaf Shaik (TU Berlin) on the study of practical privacy attacks in mobile communication
- Collaboration with Matteo Maffei (Univ Wien) on type systems for e-voting systems
- Collaboration with Bogdan Warinschi (Univ Bristol) on defining game-based privacy for e-voting protocols
- Collaboration with Robert Künnemann (CISPA, Germany) on the development of the SAPIC tool
- Collaboration with Gilles Barthe (MPI for Security and Privacy, Germany) on the automation of computer-aided cryptographic proofs
- Collaboration with Paliath Narendran's group (SUNY Albany) on automated deduction
- Collaboration with Serdar Erbatur (LMU, Germany) and Andrew Marshall (Univ Mary Washington, USA) on decision procedures for combined equational theories
- Collaboration with Hanifa Boucheneb's group (Polytechnique Montreal) on model-checking of collaborative systems
- Collaboration with John Mullins's group (Polytechnique Montreal) on information hiding

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- Bogdan Warinschi (Univ Bristol), November 2018 and April 2019.
- Ralf Sasse (ETH Zurich), November 2019.

PRIVATICS Project-Team

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. AMNECYS

- Title: AMNECYS
- Duration: 2015 - .
- Coordinator: CESICE, UPMF.
- Others partners: Inria/Privatics and LIG/Moais, Gipsa-lab, LJK, Institut Fourier, TIMA, Vérimag, LISTIC (Pole MSTIC) .
- Abstract: Privatics participates to the creation of an Alpine Multidisciplinary NEtwork on CYbersecurity Studies (AMNECYS). The academic teams and laboratories participating in this project have already developed great expertise on encryption technologies, vulnerabilities analysis, software engineering, protection of privacy and personal data, international & European aspects of cybersecurity. The first project proposal (ALPEPIC ALPs-Embedded security: Protecting Iot & Critical infrastructure) focuses on the protection of the Internet of Things (IoT) and Critical Infrastructure (CI).

7.1.2. Data Institute

- Title: Data Institute UGA
- Duration: 2017 - .
- Coordinator: TIMC-IMAG.
- Others partners: AGEIS, BIG, CESICE, GIN, GIPSA-lab, IAB, IGE, IPAG, LAPP, LARHRA, LIDILEM, LIG, LISTIC, LITT&ArTS, LJK, LUHCIE, LECA, OSUG, PACTE, TIMC-IMAG
- Abstract: Privatics is leading the WP5 (Data Governance, Data Protection and Privacy). This action (WP5) aims to analyze, in a multi-disciplinary perspective, why and how specific forms of data governance emerge as well as the consequences on the interaction between the state, the market and society. The focus will be on the challenges raised by the collection and use of data for privacy, on the data subjects' rights and on the obligations of data controllers and processors. A Privacy Impact/Risk assessments methodology and software will be proposed. A case study will focus on medical and health data and make recommendations on how they should be collected and processed.

7.1.3. CyberAlps

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

7.1.4. Antidot

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

7.1.5. DARC

- Title: DARC - the Data Anonymization and Re-identification Competition
- Type: Innovation Pédagogique - IDEX LYON
- Duration: September 2019 - 2020.
- Coordinator: INSA.
- Abstract: In order to increase awareness and empower future digital engineers in a fun way on privacy issues, the DARC project offers learning through play through a challenge carried out jointly by three different training courses of INSA students in Bourges and in Lyon. This challenge consists first of all in anonymizing a dataset from an online sales site, then secondly in trying to re-identify the anonymized data of the other groups.

7.2. National Initiatives

7.2.1. ADT PRESERVE

- Title: PRESERVE: Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE
- Duration: 2019 - 2020
- Coordinator: INSA.
- Abstract: The goal of this project is to develop a web platform to increase the user awareness on privacy issues. This platform will gather multiple works investigated in the team and will be used to conduct demonstration and stimulate new collaborations and dissemination actions to end users and media.

7.2.2. ANR

7.2.2.1. CISC

Title: Certification of IoT Secure Compilation.

Type: ANR.

Duration: April 2018 - March 2022.

Coordinator: Inria INDES project-team (France)

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

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

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

7.2.2.2. SIDES 3.0

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

Type: ANR.

Duration: August 2017 - August 2020.

Coordinator: Uness (France).

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

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

7.2.2.3. DAPCODS/IOTics

Title: DAPCODS/IOTics.

Type: ANR 2016.

Duration: May 2017 - Dec. 2020.

Coordinator: Inria PRIVATICS.

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

Abstract:

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

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

- by analyzing the inner working of a significant set of connected devices in terms of personal information leaks. This will be made possible by analyzing their data flows (and associated smartphone application if applicable) from outside (smartphone and/or Wifi network) or inside, through ondevice static and dynamic analyses. New analysis methods and tools will be needed, some of them leveraging on previous works when applicable;

- by studying the device manufacturers' privacy policies along several criteria (e.g., accessibility, precision, focus, privacy risks). In a second step, their claims will be compared to the actual device behavior, as observed during the test campaigns. This will enable an accurate and unique ranking of connected devices;
- by understanding the underlying ecosystem, from the economical viewpoint. Data collected will make it possible to define the blurred boundaries of personal information market, a key aspect to set up an efficient regulation;
- and finally, by proposing a public website that will rank those connected devices and will inform citizens. We will then test the impact of this information on the potential change of behavior of stakeholders.

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

7.2.3. Inria-CNIL collaboration

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

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

7.3. European Initiatives

7.3.1. Collaborations in European Programs, Except FP7 & H2020

7.3.1.1. UPRISE-IoT

Title: User-centric PRIvacy & Security in IoT

Programm: CHISTERA

Duration: December 2016 - December 2019

Coordinator: SUPSI (Suisse)

Inria contact: Claude Castelluccia

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

7.3.1.2. SPARTA

Title: Strategic Programs for Advanced Research and Technology in Europe (SPARTA)

Programm: H2020-SU-ICT-03-2018

Duration: February 2019 - January 2022

Coordinator: CEA

Inria contact: Thomas Jensen (Inria), Vincent Roca (for PRIVATICS)

SPARTA Cybersecurity European Competence Network. The consortium consists of 44 partners from 14 different countries, with the goal to demonstrate the setup and assessment of a European SPARTA Cybersecurity Competence Network.

7.4. International Initiatives

7.4.1. DATA

Title: Data and Algorithmic Transparency and Accountability

International Partner (Institution - Laboratory - Researcher):

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

Start year: 2018

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

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

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

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Jeremy Decouchant (University of Luxembourg) visited Privatics from 14/10/2019 to 25/10/2019 through the Erasmus Staff Mobility For Teaching program. During the visit, Jeremie Decouchant participated in network programming lectures and practical sessions at the INSA Lyon engineering school at the M1 level. In addition, the existing scientific collaborations with the team have been also extended around the usage of Intel Software Guard Extensions (SGX) to implement a privacy-preserving recommendation systems and genome studies.
- Gergely Acs, assistant professor at Budapest University (Hungary), visited our team in June. He worked together with Claude Castelluccia on the security and privacy of Federated machine learning.
- Rosin Claude Ngueveu (UQAM) visited the team in Lyon in July 2019 for two weeks to increase the DATA collaboration. During the visit, Rosin Claude Ngueveu presented joint work at APVP 2019 and advanced existing collaboration to include fairness in our work on protection of motion sensor data.

PROSECCO Project-Team

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

9.1.1.1. AnaStaSec

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

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

Duration: January 2015 - September 2019.

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

Participant: Bruno Blanchet

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

9.1.1.2. AJACS

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

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

Duration: October 2014 - March 2019.

Coordinator: Alan Schmitt, Inria (France)

Participants: Karthikeyan Bhargavan, Bruno Blanchet, Nadim Kobeissi

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

9.1.1.3. SafeTLS

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

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

Duration: October 2016 - September 2020

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

Participants: Karthikeyan Bhargavan

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

9.1.1.4. TECAP

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

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

Duration: January 2018 - December 2021

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

Participants: Bruno Blanchet, Benjamin Lipp

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

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

9.2.1.1. ERC Consolidator Grant: CIRCUS

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

Duration: April 2016 - March 2021

Coordinator: Karthikeyan Bhargavan, Inria

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

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

9.2.1.2. ERC Starting Grant: SECOMP

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

Duration: Jan 2017 - December 2021

Coordinator: Catalin Hritcu, Inria

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

9.2.1.3. NEXTLEAP (304)

Title: NEXTLEAP: NEXT generation Legal Encryption And Privacy

Programm: H2020

Duration: January 2016 - December 2018

Coordinator: Harry Halpin, Inria

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

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

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

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

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

9.3.2. Participation in Other International Programs

9.3.2.1. SSITH/HOPE

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

Program: DARPA SSITH

Duration: December 2017 - February 2021

Coordinator: Charles Stark Draper Laboratory

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

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

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

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

9.3.2.2. Everest Expedition

Program: Microsoft Expedition and MSR-Inria Collaborative Research Project

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

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

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

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

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

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

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

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

https://project-everest.github.io

9.4. International Research Visitors

9.4.1. Visits of International Scientists

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

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

9.4.1.1. Internships

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

9.4.2. Visits to International Teams

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

TAMIS Project-Team

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR

- ANR MALTHY, Méthodes ALgébriques pour la vérification de modèles Temporisés et HYbrides, Thao Dang, 4 years, Inria and VISEO and CEA and VERIMAG
- ANR COGITO, Runtime Code Generation to Secure Devices, 3 years, Inria and CEA and ENSMSE and XLIM.
- ANR AHMA, Automated Hardware Malware Analysis, 3,5 years, JCJC.

8.1.2. DGA

- PhD grant for Nisrine Jafri (2016–2019),
- PhD grant for Lamine Noureddine (2017-2020)
- PhD grant for Christophe Genevey Metat (2018-2021)
- PhD grant for Cassius De Oliveira Puodzius (2019-2022)

8.2. European Initiatives

8.2.1. ENABLE-S3 (352)

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

Program: H2020

Duration: 05/2016 - 04/2019

Coordinator: Avl List Gmbh (Austria)

Partners:

Aalborg Universitet (Denmark); Airbus Defence And Space Gmbh (Germany); Ait Austrian Institute Of Technology Gmbh (Austria); Avl Deutschland Gmbh (Germany); Avl Software And Functions Gmbh (Germany); Btc Embedded Systems Ag (Germany); Cavotec Germany Gmbh (Germany); Creanex Oy(Finland); Ceske Vysoke Uceni Technicke V Praze (Czech Republic); Deutsches Zentrum Fuer Luft - Und Raumfahrt Ev (Germany); Denso Automotive Deutschland Gmbh (Germany); Dr. Steffan Datentechnik Gmbh (Austria); Danmarks Tekniske Universitet (Denmark); Evidence Srl (Italy); Stiftung Fzi Forschungszentrum Informatik Am Karlsruher Institut Fur Technologie (Germany); Gmv Aerospace And Defence Sa (Spain); Gmvis Skysoft Sa (Portugal); Politechnika Gdanska (Poland); Hella Aglaia Mobile Vision Gmbh (Germany); Ibm Ireland Limited (Ireland); Interuniversitair Micro-Electronica Centrum (Belgium); Iminds (Belgium); Institut National De Recherche Eninformatique Et Automatique (France); Instituto Superior De Engenharia Do Porto (Portugal); Instituto Tecnologico De Informatica (Spain); Ixion Industry And Aerospace Sl (Spain); Universitat Linz (Austria); Linz Center Of Mechatronics Gmbh (Austria); Magillem Design Services Sas (France); Magneti Marelli S.P.A. (Italy); Microeletronica Maser Slspain); Mdal (France); Model Engineering Solutions Gmbhgermany); Magna Steyr Engineering Ag & Co Kg (Austria); Nabto Aps (Denmark); Navtor As (Norway); Nm Robotic Gmbh (Austria); Nxp Semiconductors Germany Gmbh(Germany); Offis E.V.(Germany); Philips Medical Systems Nederland Bvnetherlands); Rohde & Schwarz Gmbh&Co Kommanditgesellschaft(Germany);

Reden B.V. (Netherlands); Renault Sas (France); Rugged Tooling Oyfinland); Serva Transport Systems Gmbh(Germany); Siemens Industry Software Nvbelgium); University Of Southampton (Uk); Safetrans E.V. (Germany); Thales Alenia Space Espana, Saspain); Fundacion Tecnalia Research & Innovationspain); Thales Austria Gmbh (Austria); The Motor Insurance Repair Researchcentre (Uk); Toyota Motor Europe (Belgium); Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (Netherlands); Ttcontrol Gmbh (Austria); Tttech Computertechnik Ag (Austria); Technische Universiteit Eindhoven (Netherlands); Technische Universitat Darmstadt (Germany); Technische Universitaet Graz (Austria); Twt Gmbh Science & Innovation (Germany); University College Dublin, National University Of Ireland, Dublin (Ireland); Universidad De Las Palmas De Gran Canaria (Spain); Universita Degli Studi Di Modena E Reggio Emilia (Italy); Universidad Politecnica De Madrid (Spain); Valeo Autoklimatizace K.S. (Czech Republic); Valeo Comfort And Driving Assistance (France); Valeo Schalter Und Sensoren Gmbh (Germany); Kompetenzzentrum - Das Virtuelle Fahrzeug, Forschungsgesellschaft Mbh (Austria); Vires Simulationstechnologie Gmbh (Germany); Teknologian Tutkimuskeskus Vtt Oy (Finland); Tieto Finland Support Services Oy (Finland); Zilinska Univerzita V Ziline (Slovakia);

Inria contact: Olivier Zendra

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

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

In 2019, in TAMIS, Olivier Zendra and Eduard Baranov were involved in this project. The project supported one postdoc in TAMIS starting in 2017.

8.2.2. TeamPlay (653)

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

Program: H2020

Duration: 01/2018 - 12/2020

Coordinator: Inria

Partners:

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

Inria contact: Olivier Zendra

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

The permanent members of TAMIS who are involved are Olivier Zendra and Annelie Heuser.

8.2.3. SUCCESS

Title: SUCCESS: SecUre aCCESSibility for the internet of things

Program: CHIST-ERA 2015

Duration: 10/2016 - 10/2019

Coordinator: Middlesex University (UK)

Partners:

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

Inria contact: Ioana Cristescu

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

Within SUCCESS, the contribution of the TAMIS team consists in a framework for analyzing the security of a given IOT system, and notably whether it resists to attack. Our approach is to build a high-level model of the system, including its vulnerabilities, as well as an attacker. We represent

the set of possible attacks using an attack tree. Finally, we evaluate the probability that an attack succeeds using Statistical Model Checking.

In 2019, in the TAMIS team, Delphine Beaulaton, Najah Ben Said, Ioana Cristescu and Olivier Zendra were involved in this project.