RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2018

Section Highlights of the Team

Edition: 2019-03-07

ARIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Damien Stehlé was nominated IUF junior member.

5.1.2. Book

Publication of the second edition of the “Handbook of Floating-Point Arithmetic” [43].
BEST PAPERS AWARDS :
[42]
G. VILLARD.*On Computing the Resultant of Generic Bivariate Polynomials*, in "ISSAC 2018, 43rd International Symposium on Symbolic and Algebraic Computation, New York, USA, July 16-19, 2018", New York, United States, July 2018, https://hal.archives-ouvertes.fr/hal-01921369

AROMATH Project-Team (section vide)

CARAMBA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Several Invited talks: Pierrick Gaudry was an invited speaker at the ECC 2018 workshop (Osaka, Japan); Emmanuel Thomé was an invited speaker at the ANTS-XIII conference in Madison, WI, USA (The biennial ANTS conference is the main international conference on algorithmic number theory); Paul Zimmermann was an invited speaker at the 75th anniversary celebration of the journal *Mathematics of Computation* (Providence, RI, USA).
- Cécile Pierrot was awarded the DGA (Direction Générale de l'Armement) Prize from Florence Parly, the Minister of the Armed Forces, for her PhD Thesis.

BEST PAPER AWARD :
[11]
M. SCOTT, A. GUILLEVIC.*A New Family of Pairing-Friendly elliptic curves*, in "International Workshop on the Arithmetic of Finite Fields - WAIFI", Bergen, Norway, L. BUDAGHYAN, F. RODRIGUEZ-HENRIQUEZ (editors), June 2018, https://hal.inria.fr/hal-01875361

CASCADE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- Melissa Rossi received a 2018 Google's WomenTechmakers Scholarship.

DATASHAPE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Books

- Jean-Daniel Boissonnat, Frédéric Chazal, Mariette Yvinec. *Geometric and Topological Inference*. Cambridge Texts in Applied Mathematics, vol. 57, Cambridge University Press, 2018.

5.1.2. Awards

- Mathieu Carrière was awarded the Prix de thèse solennel Thiessé de Rosemont / Schneider in Mathematics by the Chancellerie des Universités de Paris for his Ph.D. work under Steve Oudot's supervision (Ph.D. funded by ERC grant Gudhi), December 2018.

GAIA Team

5. Highlights of the Year

5.1. Highlights of the Year

Computer Algebra in Scientific Computing

The GAIA team organized the conference *Computer Algebra in Scientific Computing* (CASC), University of Lille, 17–21 September 2018.

GAMBLE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Given a set of possibly intersecting polygons in 3D, we presented a breakthrough result on the problem of computing a set of interior-disjoint triangles whose geometry is close to that of the input and such that the output vertices have coordinates of fixed precision, typically integers or floating-point numbers of bounded precision (eg. int, float, double). This problem is important in academic and industrial contexts because many 3D digital models contain self intersections and many applications require models without self intersections. Despite the theoretical and practical relevance of this problem, there was almost no literature on the subject and we presented its first satisfactory solution [12].

GRACE Project-Team (section vide)

LFANT Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Chloe Martindale defended her PhD thesis on *Isogeny Graphs, Modular Polynomials, and Applications*.

Antonin Riffaut defended his PhD thesis on *Effective computation of special points*.

A new release of PARI/GP, 2.11.0, has been published. This is a major stable release ending a development cycle which started in November 2016; it includes among others an extensive new package for modular forms.

2018 was also a year with more workshops on PARI/GP than ever: Besides two general workshops uniting developers and users, organised together with the universities of Besançon and Rome in the respective cities, the team participated with lectures on PARI/GP at the École jeunes chercheurs en théorie des nombres à Besançon (https://indico.math.cnrs.fr/event/2735/) and at the summer school ZETAS 2018 at Le Bourget du Lac (https://etzetas2018.sciencesconf.org/).

OURAGAN Team

5. Highlights of the Year

5.1. Highlights of the Year

- In [24], Antonin Guilloux and Julien Marché propose a closed formula for the Mahler measure of a class of bivariate polynomials with rational coefficients (exact polynomials). This class of polynomials contains A-polynomials of knot complements and the authors express the Mahler Measure of a volume function defined on the vanishing set of the polynomial.

  As computing Mahler measures is a well known challenge in number theory and as computing volumes of knots complements is a critical objective for our research on character varieties, this result make an original bridge between our two main research directions.
- A key encapsulation message named Mersenne-756839 has been submitted at the NIST call for standard on Post-Quantum Cryptography. This submission is a complement to the article [13] presented in three invited lectures by Antoine Joux (JFLI (UMI CNRS) / Tokyo university , Nanyang Technological University, LATtice Crypto and Algorithms conference).
- Our agreement with WATERLOO MAPLE INC. has been reviewed for a two years term in 2018. Out next objective is the diffusion of our new solver for univariate polynomials with real coefficients.

POLSYS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Jean-Charles Faugère and Ludovic Perret received the Atos-Joseph Fourier 2018 prize [0] for their project on Quantum Safe Security.

[0] https://atos.net/fr/2018/communiques-de-presse_2018_07_06/atos-et-genci-annoncent-les-laureats-du-prix-atos-joseph-fourier-2018

SECRET Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- **Keynote at Eurocrypt:** A. Canteaut bas been an invited keynote speaker at Eurocrypt 2018 in Tel-Aviv.
- **Cryptanalysis of candidates to the NIST post-quantum competition:** The members of the project-team are involved in the design of several attacks against submissions to the NIST standardization effort for post-quantum cryptography. This work has led to the break of `EDON-K` key encapsulation mechanism, of `RLCE` encryption scheme, of `RankSign`, and of a recently proposed IBE scheme.
- **Quantum fault-tolerance with constant overhead:** In a couple of papers published at STOC 2018 and FOCS 2018, A. Grospellier and A. Leverrier together with O. Fawzi (from ENS Lyon) proved that quantum expander codes can be combined with quantum fault-tolerance techniques to achieve constant overhead: the ratio between the total number of physical qubits required for a quantum computation with faulty hardware and the number of logical qubits involved in the ideal computation is asymptotically constant, and can even be taken arbitrarily close to 1 in the limit of small physical error rate. This improves on the polylogarithmic overhead promised by the celebrated threshold theorem.

SPECFUN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Georges Gonthier, Martìn Abadi and Cédric Fournet receiver the 20 year test-of-time award for their LICS 1998 paper *Secure Implementation of Channel Abstractions*, during LICS 2018 in Oxford.

CAIRN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Petr Dobias received the A. Richard Newton Young Fellow Award at IEEE/ACM Design Automation Conference (DAC), San Francisco, 2018.

Davide Pala received the A. Richard Newton Young Fellow Award at IEEE/ACM Design Automation Conference (DAC), San Francisco, 2018.

CAMUS Team

5. Highlights of the Year

5.1. Highlights of the Year

Bérenger Bramas, Inria Research Scientist, has joined the team in September 2018.
Matthew Wahab, Inria Research Engineer, has joined the team in August 2018.

CASH Team

5. Highlights of the Year

5.1. Highlights of the Year

- CASH has been validated as a *équipe projet commune* (EPC) by the *comité des projets*.
- We designed a dataflow transformation which always recovers all the FIFO in our dataflow model (DPN) after a loop tiling [1], [9], a program transformation widely used in automatic parallelization. This is an important enabling transformation which reinforces DPN as an intermediate representation in the CASH HLS project.
- We obtained new results on the comparison between different forms of synchronisation on futures, bringing a better understanding on the impact dataflow synchronisation and future typing on program synchronisation.

CORSE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- Christodoulis, G., Broquedis, F., Muller, O., Selva, M., Desprez, F., *An FPGA target for the StarPU heterogeneous runtime system*. ReCoSoC 2018

BEST PAPERS AWARDS :
[25]
G. CHRISTODOULIS, M. SELVA, F. BROQUEDIS, F. DESPREZ, O. MULLER.*An FPGA target for the StarPU heterogeneous runtime system*, in "13th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (RECOSOC 2018)", Lille, France, IEEE, July 2018, p. 1-8, http://hal.univ-grenoble-alpes.fr/hal-01858951

PACAP Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

André Seznec won the three tracks of the 1st Championship of Value Prediction with the EVES predictor.

Arthur Perais, former PhD student in the project-team, and André Seznec received the best paper award at the conference ACM PACT 2018 for their paper “Cost Effective Speculation with the Omnipredictor”.

BEST PAPERS AWARDS :

[39]

A. SEZNEC.*Exploring value prediction with the EVES predictor*, in "CVP-1 2018 - 1st Championship Value Prediction", Los Angeles, United States, June 2018, p. 1-6, https://hal.inria.fr/hal-01888864

[35]

A. PERAIS, A. SEZNEC.*Cost Effective Speculation with the Omnipredictor*, in "International conference on Parallel Architectures and Compilation Techniques (PACT ’18),", Limassol, Cyprus, November 2018 [*DOI :* 10.1145/3243176.3243208], https://hal.inria.fr/hal-01888884

AOSTE2 Team

5. Highlights of the Year

5.1. Highlights of the Year

This is the last activity report of the team AOSTE2 since it ends in 2018.

The ATT StatInf project, prepared by Liliana Cucu-Grosjean and Adriana Gogonel has been accepted in July 2018. The associated start-up creation has been selected for participation to the Digital Start-up program (jointly supported by EMLyon and Inria). The start-up will be created beginning of 2019 by Adriana Gogonel, Cristian Maxim and Liliana Cucu-Grosjean as founding members.

HYCOMES Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

The highlights of the year are:

- The start of two industrial collaborations of crucial importance for the Hycomes team: (i) the FUI ModeliScale project, in the context of which the Hycomes team design novel algorithms for the structural analysis of multimode DAE systems, with the objective of supporting a larger class of multimode Modelica models; and (ii) the Glose project, in collaboration with Safran Tech., on the topics of cyber-physical systems modeling and cosimulation.
- Albert Benveniste, Benoît Caillaud and co-authors have published a book on contract-based reasoning for cyber-physical systems design. This book is the result of more than 10 years of research on contract and interface theories.
- Albert Benveniste, Benoît Caillaud and co-authors have published a paper in *The Proceedings of the IEEE* on the design of Hybrid Systems modeling languages, based on our past work on ODE-based synchronous languages (namely the Zélus language).

KAIROS Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

BEST PAPERS AWARDS :
[16]
A. SCHULZ-ROSENGARTEN, R. VON HANXLEDEN, F. MALLET, R. DE SIMONE, J. DEANTONI.*Time in SCCharts*, in "Forum on specification & Design Languages", Munich, Germany, September 2018, p. 5-16, Best Paper Award [*DOI :* 10.1109/FDL.2018.8524111], https://hal.inria.fr/hal-01898285

PARKAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Guillaume Baudart was awarded the **ACM SIGBED Paul Caspi Memorial Dissertation Award** for his thesis “A Synchronous Approach to Quasi-Periodic Systems” [27] prepared in the PARKAS Team under the supervision of Marc Pouzet and Timothy Bourke and defended in 2017.

SPADES Project-Team (section vide)

TEA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Inria created a new International Chair in collaboration with Insa-Rennes and appointed American computer engineer Shuvra Bhattacharyya, Professor at the University of Maryland, to the part-time position. Shuvra will hold the International Chair for a period of five years, fostering our joint collaboration with the CNRS-Insa laboratory IETR.

TEA becomes the first Inria group to host two International Chairs: last year, Rajesh Gupta, Director of UC San Diego Data Science Institute, was appointed Inria International Chair with project-team TEA.

Jean-Pierre Talpin spent the first semester to prepare an ERC advanced grant. He also gave a keynote presentation at the FDL'18 conference on "refinement types for system design".

Thierry Gautier and Albert Benveniste gave an invited seminar at the Collège de France in Gérard Berry's 2017-2018 lecture course [15].

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team

3. Highlights of the Year

3.1. Highlights of the Year

3.1.1. Awards

- The ERC Consolidator grant VESTA on verified static analysis was awarded to David Pichardie and launched in September 2018.
- The ANR project SCRYPT led by Frédéric Besson was accepted and starts in February 2019.

BEST PAPERS AWARDS :
[19]
A. SALIM AL-SIBAHI, A. S. DIMOVSKI, T. JENSEN, A. WASOWSKI.*Verification of High-Level Transformations with Inductive Refinement Types*, in "GPCE 2018 - 17th International Conference on Generative Programming: Concepts & Experience", Boston, United States, November 2018, p. 1-14, https://hal.inria.fr/hal-01898058

CONVECS Project-Team (section vide)

DEDUCTEAM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Logipedia

We have launched in September the first system independent encyclopedia of formal proofs: LOGIPEDIA.

Awards

Serge Abiteboul and Gilles Dowek have received the Award *La science se livre* in January.

GALLINETTE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Creation and new permanents members

The team has been created as a project team on June 2018. Two new permanent members have joined the team:

- Guilhem Jaber, as an assistant professor of the University of Nantes (September 2018).
- Pierre-Marie Pédrot as an Inria researcher (October 2018).

4.1.2. Awards

BEST PAPERS AWARDS :

[7]

N. TABAREAU, É. TANTER, M. SOZEAU.*Equivalences for Free: Univalent Parametricity for Effective Transport*, in "Proceedings of the ACM on Programming Languages", September 2018, p. 1-29 [*DOI :* 10.1145/3234615], https://hal.inria.fr/hal-01559073

[14]

É. MIQUEY.*A sequent calculus with dependent types for classical arithmetic*, in "LICS 2018 - 33th Annual ACM/IEEE Symposium on Logic in Computer Science", Oxford, United Kingdom, LICS '18 Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, ACM, July 2018, p. 720-729, https://arxiv.org/abs/1805.09542 [*DOI :* 10.1145/3209108.3209199], https://hal.inria.fr/hal-01703526

GALLIUM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

In 2018, Xavier Leroy received the “Grand prix” jointly awarded by Inria and Académie des sciences.

Gergö Barany received the Best Paper Award for the paper “Finding Missed Compiler Optimizations by Differential Testing” [19] at the 27th International Conference on Compiler Construction (CC 2018).

MARELLE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

The paper by Barthe, Grégoire, and Laporte at *Computer Security Foundations* on cryptographic constant-time was awarded a distinguished paper award.
BEST PAPERS AWARDS :
[16]
G. BARTHE, B. GRÉGOIRE, V. LAPORTE.*Secure Compilation of Side-Channel Countermeasures: The Case of Cryptographic "Constant-Time"*, in "CSF 2018 - 31st IEEE Computer Security Foundations Symposium", Oxford, United Kingdom, July 2018, https://hal.archives-ouvertes.fr/hal-01959560

MEXICO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Reaching agreement in unstable times

Reaching approximate agreement in a distributed system among a set of local input values is a problem that often is repeatedly solved in artificial and natural distributed systems. Time efficient algorithms for this problem are thus of great theoretical and practical relevance. In [28] we studied the performance of such algorithms in dynamic networks. We showed lower time complexity bounds, demonstrating that already relatively simple broadcast and averaging algorithms achieve optimal time complexity. The results also imply new tight lower time complexity bounds for approximate agreement in classic distributed computing models with stable network architectures; solving a previously open problem.

5.1.2. New Semantics and State Spaces for Biological networks (and beyond)

We have gained major new insights into the dynamics of biological networks by

- obtaining [34], on the one hand, bi-directional translations between Contextual nets and BNs and correspondences between results on synchronism sensitivities. Taking advantage of CPN semantics enabling more behaviour than the generalized asynchronous updating mode, we propose an encoding of BNs that ensures correct abstraction of any multivalued refinement; and
- [20], [32] investigating update modes for discrete networks. It is commonly expected that Boolean networks produce an over-approximation of behaviours (reachable configurations), and that subsequent refinements would only prune some impossible transitions. However, we show that even generalized asynchronous updating of Boolean networks, which subsumes the usual updating modes including synchronous and fully asynchronous, does not capture all transitions doable in a multivalued or timed refinement. We introduce a new semantics for interpreting BNs which meets with a correct abstraction of any multivalued refinements, with any update mode. This semantics subsumes all the usual updating modes, while enabling new behaviours achievable by more concrete models. Moreover, it appears that classical dynamical analyses of reachability and attractors have a simpler computational complexity: – reachability can be assessed in a polynomial number of iterations (instead of being PSPACE-complete with update modes); – attractors are hypercubes, and deciding the existence of attractors with a given upper-bounded dimension is in NP (instead of PSPACE-complete with update modes). The computation of iterations is in NP in the very general case, and is linear when local functions are monotonic, or with some usual representations of functions of BNs (binary decision diagrams, Petri nets, automata networks, etc.). In brief, the most permissive semantics of BNs enables a correct abstract reasoning on dynamics of BNs, with a greater tractability than previously introduced update modes. These works open new perspectives in concurrent semantics, and at the same time will allow to capture hitherto inaccessible phenotypes and pathways in biological networks.

5.1.3. Awards

-

MOCQUA Team

5. Highlights of the Year

5.1. Highlights of the Year

Completeness of the ZX-Calculus

We have proved this year the completeness of the ZX-calculus. The completeness of the ZX-calculus was the main open question in the field of categorical quantum mechanics and was open for about 10 years. This results has been published at LiCS'18 [17], [16] and also presented at TQC'18 and QIP'19, the main two conferences in quantum information processing.

PARSIFAL Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

D. Miller has been made General Chair of the LICS Conference Series for three years, starting July 2018.

PI.R2 Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Matthieu Sozeau received a Distinguished Paper award at ICFP 2018 for his work on "Equivalences for Free!"[36], together with co-authors Nicolas Tabareau and Eric Tanter.

Amina Doumane received in January 2018 the best paper award given by *La Recherche* for her paper in LICS 2017 entitled *Constructive Completeness for the Linear-Time mu-Calculus* for which she already received the Kleene Award from the LICS conference in 2017.

Amina Doumane received the Ackermann Award from the EACSL committee. As a result, she was invited to give a lecture at CSL 2018.

SUMO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- The ANR project TickTac led by Ocan Sankur was accepted and starts in March 2019.
- New partnership with Mitsubishi Electric (MERCE): one PhD thesis started in Fall 2018, and a member of MERCE will be hosted by SUMO in 2019.

5.1.1. Awards

BEST PAPERS AWARDS :
[11]
G. BACCI, P. BOUYER, U. FAHRENBERG, K. G. LARSEN, N. MARKEY, P.-A. REYNIER.*Optimal and Robust Controller Synthesis: Using Energy Timed Automata with Uncertainty*, in "FM 2018 - International Symposium on Formal Methods", Oxford, United Kingdom, LNCS, Springer, July 2018, vol. 10951, p. 203-221 [*DOI :* 10.1007/978-3-319-95582-7_12], https://hal.archives-ouvertes.fr/hal-01889222

TOCCATA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

J.-C. Filliâtre served as judge at the ICPC regional programming contests SWERC 2017 and 2018. These two editions were organized in Paris and gathered each year 80 teams of three students from universities and schools from South-West Europe. https://swerc.eu/

The 2nd edition of the Handbook of Floating-Point arithmetic was published [28]

5.1.1. Awards

R. Rieu-Helft received the "Student Gold Medal" award, and J.-C. Filliâtre the "Best challenge submitted" award, at the *VerifyThis@ETAPS2018 verification competition*http://www.pm.inf.ethz.ch/research/verifythis/Prizes.html

VERIDIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Marie Duflot-Kremer received the Serge Hocquenghem prize awarded biannually by *Association pour l'Innovation Didactique* for her contributions to the popularization of computer science and in particular her work on developing and promoting unplugged computer science activities.

Thomas Sturm was a plenary invited speaker at ISSAC 2018, the leading conference in Symbolic Computation.

CIDRE Project-Team (section vide)

COMETE Project-Team (section vide)

DATASPHERE Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Kavé Salamatian has been awarded in 2018 a President's International Fellowship of the Chinese Academy of Sciences.

PESTO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Analysis of the 5G Standard

The work on the security analysis of the upcoming 5G mobile phone standard presented at CCS'18 [13] was acknowledged in the GSMA "Mobile Security Research Hall of Fame" and picked up by media in France, Switzerland and the UK (Daily Mail, 20 Minutes, Est Républicain, Tagesanzeiger, CNRS Le Journal, etc.).

5.1.1. Awards

BEST PAPERS AWARDS :
[18]
V. CHEVAL, S. KREMER, I. RAKOTONIRINA.*DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice*, in "39th IEEE Symposium on Security and Privacy", San Francisco, United States, May 2018, https://hal.inria.fr/hal-01763122

PRIVATICS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Cédric Lauradoux, Vincent Roca with the participation of Claude Castelluccia have created a MOOC on Privacy which has been followed this year by more than 20000 persons.

PROSECCO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- We published 20 papers at top-tier conferences and journals such as POPL (5), ICFP (2), PLDI (1), OOPSLA (1), ACM CCS (1), IEEE S&P (1), IEEE CSF (1), TOPLAS (1), and JCS (1).
- The HACL* verified cryptographic library developed in our group was integrated by Linux (WireGuard) and Tezos, and more verified crypto primitives were integrated in Mozilla Firefox.
- We organized a Dagstuhl Seminar on Secure Compilation (18201)
- Catalin Hritcu served as Program Chair for the Workshop on Principles of Secure Compilation at POPL'18

TAMIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Change of team leader

Participants: Olivier Zendra, Axel Legay

Olivier Zendra was appointed team leader instead of Axel Legay on 12 Oct 2018.

"Chaire Analyse de Menaces" (Threat Analysis)

Participants: Fabrizio Biondi

Fabrizio Biondi resigned from Centrale Supelec and from the "Chaire Analyse de Menaces" (Threat Analysis) on 31 Dec 2018.

TeamPlay H2020 project, coordinated by Olivier Zendra

Participants: Olivier Zendra, Cécile Bouton, Yoann Marquer, Céline Minh, Tania Richmond

Launch on Jan 2018 of the TeamPlay (https://www.teamplay-h2020.eu) H2020 project (that had been submitted 25 April 2017), about the integration of nonfunctional properties in programs. TAMIS is in charge of security properties.