
RESEARCH CENTER

FIELD
**Algorithmics, Programming, Software and Architecture**

Activity Report 2016

# Section Highlights of the Team

Edition: 2017-08-25

# ARIC Project-Team (section vide)

# AROMATH Project-Team (section vide)

**CARAMBA Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

The Caramba project-team was created on January 1st, 2016!

In October 2016, Pierrick Gaudry and Emmanuel Thomé, together with colleagues from the University of Pennsylvania (USA), have performed a discrete logarithm computation of a 1024-bit trapdoored prime [18].

**CASCADE Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Conferences*

- Hoeteck Wee is one of the invited speakers at Asiacrypt 2016.
- Michel Abdalla is one of the invited speakers at ICISC 2016.

### *5.1.2. Awards*

Romain Gay and Hoeteck Wee, together with Dennis Hofheinz and Eike Kiltz, received the Best Paper Award at Eurocrypt 2016 .
BEST PAPERS AWARDS :
[40] **Advances in Cryptology – EUROCRYPT 2016**. R. GAY, D. HOFHEINZ, E. KILTZ, H. WEE.

**DATASHAPE Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Awards*

Jean-Daniel Boissonnat has been elected a professor at the Collège de France, on the Chair Informatics and Computational Sciences for the academic year 2016-2017.

### *5.1.2. Books*

Publication of a book [29], providing a self-contained presentation of the theory of persistence modules over the real line, the objects that are at the heart of the field of TDA.

GRACE Project-Team

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Events organization*

- A. Couvreur, D. Augot and D. Lucas organized with L. De Feo and Hugues Randriambololona (ENST ParisTech) a spring school on coding and cryptology in la Chapelle Gauthier (Seine et Marne).
- A. Couvreur and D. Augot organized 4 days workshop in november 2016 for the ANR MANTA. The topics were: “Decoding” and “Codes from surfaces”.
- SageDays75. To conclude the ACTIS projet, we organized a one-week SageDays in August 2016. The day was spent at Inria Saclay, and people were staying at night in a cottage in Vallée de Chevreuse.

  The overall theme of this Sage Days was coding theory and exact linear algebra related to it, but there was be lots of general hacking. The aim of this Sage Days was to Introduce Sage to coding theorists; have presentations about the enhancements we made to Sage’s coding theory library during Inria’s ACTIS project; Help people to work on their own projects.

  We had a few talks on the mornings, and coding sprints on the afternoons. The first days’ talks were focused on basic functionalities of our library, the last 2 days on advanced functionalities, with an emphasis on Sage development.

  We were glad to attract several core sage developpers, who recognized the quality of the work done by D. Lucas.

**LFANT Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

Release of Pari 2.9 after two years of development. This stable releases includes three brand new modules ($L$-functions, Associative and Central Simple Algebras, and Modular Symbols), a major overhaul of the Elliptic Curves and Number Fields modules.

Iuliana Ciocanea-Teodorescu has defended her PhD thesis on *Algorithms for finite rings* in June 2016 http://www.theses.fr/2016BORD0121.

Pinar Kiliçer has defended her PhD thesis on *The class number one problem for genus-2 curves* in July 2016 [11].

**POLSYS Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

The goal of the RISQ project is to prepare the security industry to the upcoming shift of classical cryptography to quantum-safe cryptography. The RISQ project is a massive effort at the French level to embrace the quantum-safe revolution. The project gather 15 partners : ANSSI, C&S, CEA, Crypto Experts, EADS, ENS Lyon, ENS Paris, Gemalto, Orange, PCQC, POLSYS (Inria de Paris), Université de Rennes, Secure IC, Thales CS, and Université de Versailles.

The RISQ project is certainly the biggest (in term of number of partners, as well as funding) industrial project ever organized in quantum-safe cryptography. RISQ is one of few projects accepted in the "Grands Défis du Numérique" which is managed by BPI France, and will be funded thanks to the PIA.

POLSYS actively participated to gather the partners of RISQ, and in defining the proposal. POLSYS will lead the academic effort in RISQ.

Jointly with LAAS (D. Henrion, S. Naldi), we have released a new MAPLE library SPECTRA for finding a real point $x = (x_1, ..., x_n)$ such that the symmetric matrix $A(x) = A_0 + A_1\, x_1 + \cdots + A_n\, x_n$ is positive semidefinite using exact arithmetic (see http://homepages.laas.fr/henrion/software/spectra/).

Our open source C library SLV has been officially released this year with a presentation at ISSAC. It aims at solating and approximating the real roots of univariate polynomials with integer coefficients (see http://www-polsys.lip6.fr/~elias/soft.html)

### *4.1.1. Awards*

Matías Bender received the Distinguished Student Author Award of ISSAC2016 for his paper [22] written with J.-Ch. FAUGÈRE, L. PERRET and E. TSIGARIDAS.
BEST PAPERS AWARDS :
[22] **ISSAC '16 - 41st International Symposium on Symbolic and Algebraic Computation**. M. R. BENDER, J.-C. FAUGÈRE, L. PERRET, E. TSIGARIDAS.

**SECRET Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Post-quantum symmetric cryptanalysis*

We have been considering the problem of symmetric cryptography in the future environment that will see the arrival of quantum computers. Indeed, this environment will pose a real problem for the majority of asymmetric primitives, but little is known about the implications for the security of symmetric primitives. Confidence in our symmetric primitives is entirely based on our knowledge within the field of cryptanalysis, but in reality, we do not know much about the symmetric post-quantum attacks. If we want post-quantum systems to be reliable and efficient, we need to understand how adversaries might exploit this new computing power. This year, two preliminary results have been obtained within the team and published at CRYPTO 2016 [51] and in the *IACR Transactions on Symmetric Cryptology* [23]. They include surprising results demonstrating that, in some scenarios, some symmetric systems can also become vulnerable to the quantum computer. Recently María Naya-Plasencia has been awarded an ERC starting grant, QUASYModo, to work on this subject. This grant will enable us to continue this work in more depth.

### *5.1.2. Real-word impact of some theoretical cryptanalytic works*

Weak cryptography can be used long after weaknesses have been found by the academic community. For instance, Rogaway warned that the predictable IV used in TLS was a problem in 2002, but it took a public demonstration with a practical exploit in 2011 (the BEAST attack) for servers and clients to implement countermeasures. The same happened with the use of compression (CRIME), unsecure version fallback (POODLE), and known biases in RC4 (RC4NOMORE), to name a few examples. In joint works at NDSS and ACM CCS, K. Bhargavan from the PROSECCO project-team and G. Leurent showed two almost practical attacks against deprecated cryptographic primitives that are still used in real-world applications. The SLOTH attack targeted the use of MD5 in TLS for in-protocol signatures, and the Sweet32 attack targeted the use of 64-bit block ciphers: Blowfish in OpenVPN, and 3DES in TLS. Moreover, the SLOTH attack received a distinguished paper award at NDSS.

### *5.1.3. Symmetric ciphers for homomorphic encryption schemes*

In order to avoid the (extremely) high expansion rate of homomorphic encryption, a solution consists in transmitting to the server the ciphertext $c$ obtained by encrypting $m$ with a symmetric scheme (the corresponding secret key encrypted by the homomorphic cipher is also transmitted). The server then needs to compute $m$ encrypted with the homomorphic scheme from $c$, i.e. the server needs to homomorphically evaluate the decryption circuit of the symmetric cipher. Hybrid encryption schemes dedicated to this application then require the use of symmetric ciphers with very specific features. Our team has two important contributions on this topic: the design of new appropriate solutions based on stream ciphers [44], and the attack of a cipher proposed by Méaux et al. in this context [48], [32].

### *5.1.4. Awards*

BEST PAPERS AWARDS :

[58] **Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016**. A. PHESSO, J.-P. TILLICH.

[41] **Network and Distributed System Security Symposium – NDSS 2016**. K. BHARGAVAN, G. LEURENT.

**SPECFUN Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

### *4.1.1. Awards*

Pierre Lairez has received the *ISSAC Distinguished Paper Award* for his joint work with T. Vaccon on $p$-adic differential equations [58].

**VEGAS Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

Inria signed a contract for the integration of ISOTOP within Maple.

The project-team VEGAS will terminate at the end of 2016. A new project-team GAMBLE (Geometric Algorithms and Models Beyond the Linear and Euclidean realm) is currently submitted. It intends to extend computational geometry to non-linear objects, non-Euclidean spaces and probabilistic complexities.

CAIRN Project-Team

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Our work on accuracy evaluation and optimisation for fixed point arithmetic was presented during a tutorial "Fixed-point refinement, a guaranteed approach towards energy efficient computing" at HiPEAC Conference in January 2016 [60].
Members of CAIRN got six papers accepted at IEEE/ACM Design Automation and Test in Europe for 2017, one of the major events in design automation.

**CAMUS Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Arthur Charguéraud, Inria Research Scientist, has joined the team in October 2016.

The first release of the speculative polyhedral loop parallelizer *Apollo*[0] has been published under the BSD 3-Clause Open Source License.

### *5.1.1. Awards*

BEST PAPERS AWARDS :
[13] **Euro-Par 2016**. J. M. MARTINEZ CAAMAÑO, W. WOLFF, P. CLAUSS.

[0] http://apollo.gforge.inria.fr

**COMPSYS Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### Scientific Results and Dissemination

Despite the approaching end of Compsys, we continued the objectives we fixed for Compsys III, i.e., pushing static compilation beyond its present limits, both in terms of techniques and applications. Our most important efforts in 2016 were to extend static analysis from sequential codes to parallel specifications and languages, to develop polynomial techniques, and to increase inter-disciplinary collaborations and dissemination towards HPC users and their applications. The most important results in 2016 are the following:

- **Publications** Well recognized in the polyhedral community, we got three papers at IMPACT'16, the central event of this community, one paper at the main compiler conference (CC'16), and a last one in the field of FPGA, which remains an important target for polyhedral optimizations. See Sections 7.1 to 7.7 for more details.
- **Interdisciplinary spring school** With colleagues from HPC numerical simulation, we organized a very successful inter-disciplinary event in May 2016, to bridge the gap between polyhedral compilation and HPC users. See details in Section 10.1 .
- **Move towards HPC users** In addition to the spring school we organized, we increased our activity towards HPC users and their applications through the supervision of the internship of J. Versaci (quantum physics), the reviewing of T. Gasc's PhD thesis (fluid dynamics), and the regular contacts with the LMGC lab (mechanics).
- **PhD theses** The end of Compsys coincided also with the end of two PhD theses, the PhD thesis of Guillaume Iooss [16] and the PhD thesis of Alexandre Isoard [17], see Section 10.2.2 .
- **Final evaluation** The team was evaluated in March 2016, this was also its final evaluation.

### Final Evaluation and End of Compsys

Compsys has been created in 2002 as an Inria team, then in 2004 as an Inria project-team, and evaluated by Inria first in 2007, then in 2012. It was evaluated again in March 2016, which was its final evaluation because an Inria project-team is limited to 12 years. The construction of a new project was planned in early 2015, following the shift in the research directions that started in the second half of Compsys III. A few tentative research directions were:

- Shift the application domain from embedded systems to high performance computing (HPC) but at small scale (desktop HPC: FPGA, GPU, multicores). In fact, the two ecosystems are nowadays slowly converging.
- A stronger attention to real HPC users and real HPC applications may lead to better programming models ("putting the programmer in the loop").
- Design new models of programs. The polynomial model is but an example.
- Explore the synergy between parallel programming and program verification and certification; in particular, import approximation methods from one field to the other. Abstract interpretation is a case in point.

However, while its field of expertise, compilation for parallel and heterogeneous systems, is still of crucial importance, the unexpected departure in Sep. 2015 of two of its staff members made this future impossible. We nevertheless continued in 2016, in particular to present our activities in this last evaluation, until the three last members had to split in three different cities (Lyon, Paris, Rennes). We report here some of the comments made by the external reviewers that, we think, summarize well some aspects of our efforts, successes, and difficulties during 15 years:

- *Compsys established and matured the polyhedral optimization approach, which is the state of the art for locality and parallelism optimization in optimizing compilers. The project has had world-wide impact.*
- *We strongly recommend that the members of the team are accommodated in Camus, Cairn, Parkas, or another complementary Inria team, irrespective of the geographical location. Otherwise, Inria will lose one of its peaks of research excellence in Computer Science.*
- *This team is a prime example where Inria requirements on teams are damaging science and collaboration.*
- *This team has produced many impactful results and is considered as the Polyhedral center of excellence. It is globally recognized for its research in both front-end (polyhedral optimizations) and back-end (graph optimizations) compiler optimization techniques integrating elegant foundational theory with real implementation on various architectures (multi-core, FPGAs, DSP, GPU etc.).*
- *In back-end optimizations, the team had developed the state-of-the-art SSA and decoupled register allocation techniques that are important to achieving peak performance.*
- *They have internationally visible and impactful research in compilers, technology transfer to companies through collaborations and through start-ups. They raised the global awareness of polyhedral analysis through creation of workshops, summer schools etc., essentially reviving interest in the topic about a decade ago, and finally educating next-generation of researchers in this area, who are now contributing to both academic and industrial research landscape in France and beyond.*

- *The start-up company (XtremLogic on HLS) is an excellent concrete evidence of technology transfer from the team. [...] In the future, a more careful analysis of the trade-off between technology transfer and academic research is necessary for small project teams so that a promising research direction does not get jeopardized in Inria.*
- *The Compsys team has truly achieved research excellence in compilation techniques. Unfortunately, the future of the team remains uncertain due to administrative policies. Inria should enable the team to continue with their research strengths in polyhedral analysis and graph-theory based SSA-type optimizations.*

# CORSE Project-Team (section vide)

**DREAMPAL Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

2016 is the last year of Dreampal's existence as an Inria project-team. Due to different scientific objectives, three of the members (S. Meftali, J.L. Dekeyser, P. Marquet) will create a group within the Cristal laboratory, while the team leader V. Rusu will collaborate with the 2xs team within Cristal. Frédéric Guyomarch joined the L2EP laboratory, and external collaborator Rabie Ben Atitallah continues his activity in the LAMIH laboratory in Valenciennes.

This activity report has been written by the team leader, based on the information available to him at the time of its writing. Any activity, e.g., by other team members, not reflected in the report, is only missing because of lack of input from the people concerned.

**PACAP Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

André Seznec was elevated as an ACM Fellow in December 2016 with the citation: “For contributions to branch prediction and cache memory design”.

André Seznec won the three tracks of the 5th Championship on Branch Prediction.

### *5.1.1. Awards*

Sajith Kalathingal, Sylvain Collange, Bharath Swamy and André Seznec received the Best Paper award of the SBAC-PAD 2016 conference.

Damien Hardy, Isabelle Puaut, Yiannakis Sazeides won the best paper award of the Embedded Systems Software track at DATE 2016: Probabilistic WCET estimation in presence of hardware for mitigating the impact of permanent faults. Design, Automation and Test in Europe. Dresden, Germany, March 2016.

Aswinkumar Sridharan and André Seznec won the best paper award for “Discrete Cache Insertion Policies for Shared Last Level Cache Management on Large Multicores” at the 30th IEEE International Parallel & Distributed Processing Symposium, May 2016, Chicago.

For his PhD thesis [10] “Increasing the Performance of Superscalar Processors through Value Prediction”, Arthur Perais received:

- Prix de thèse Fondation Rennes 1, 1er Prix de l’école doctorale MATISSE;
- Prix de thèse Gilles Kahn, accessit.

BEST PAPERS AWARDS :
[46] **5th JILP Workshop on Computer Architecture Competitions (JWAC-5): Championship Branch Prediction (CBP-5)**. A. SEZNEC.
[45] **5th JILP Workshop on Computer Architecture Competitions (JWAC-5): Championship Branch Prediction (CBP-5)**. A. SEZNEC.
[36] **International Symposium on Computer Architecture and High-Performance Computing (SBAC-PAD)**. S. KALATHINGAL, S. COLLANGE, B. NARASIMHA SWAMY, A. SEZNEC.
[35] **Design, Automation and Test in Europe**. D. HARDY, I. PUAUT, Y. SAZEIDES.
[48] **30th IEEE International Parallel & Distributed Processing Symposium**. A. SRIDHARAN, A. SEZNEC.

**TASC Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Awards*

Award at the MiniZinc Challenge 2016 solver competition in the Fixed category (Bronze). The aim of the challenge is to start to compare various constraint solving technology on the same problems sets. The focus is on finite domain propagation solvers. An auxiliary aim is to build up a library of interesting problem models, which can be used to compare solvers and solving technologies.

# AOSTE Project-Team (section vide)

# CONVECS Project-Team (section vide)

**HYCOMES Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Team members have made a significant step towards the definition of a formal semantics of multimode DAE systems, their strucutral analysis and the generation of simulation code. In particular, impulsive behavior at mode changes are handled correctly [19] (see Section 7.1 for full details). This semantics has been implemented, in part, in the SunDAE prototype software (Section 6.1 ).

**MUTANT Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

### Startup Creation

Arshia Cont with José Echeveste and Philippe Cuvillier (former PhD students) are creating a Startup around Antescofo to bring the product to greater public starting March 2016 http://antescofo.com. The project is hosted by the French Incubator AgoraNov.

It was awarded the “Emergence Award” in 2015 that help emerging new technology companies to study the project, and an i-LAB prize in 2016, supported by the French Ministry of Culture and Bpifrance, and it has been a finalist of the Midemlab 2016.

**PARKAS Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

### *4.1.1. Awards*

Marc Pouzet won the Inria/French Académie des Sciences/Dassault Systèmes Innovation award.

**POSET Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

An $\alpha$-version of the T-calculus [21] have been released [0].

It has been experimented in an Art & Science project [0] that have illustrated its expressiveness and simplicity for describing reactive music [19], [23]. This Art & Science project will be "on stage" in february 2017 via a "Duo solo for piano and computer".

The software *i-score* have also been further experimented [24], [16] especially during the visit of Shlomo Dubnov (UCSD) in 2016.

[0] see the T-calculus url
[0] see the Interpolation project

# SPADES Project-Team (section vide)

**TEA Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

In 2016, TEA was successfully evaluated, one year after its creation. The team started fruitful collaborations with UC San Diego, with Mitsubishi R&D, with ASTRI, to elaborate our research program on system composition, verification, and simulation toward novel applications perspectives in codesign, operating system design, factory automation, robotics.

**ANTIQUE Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

The team obtained several strong results published in excellent international conferences, with high theoretical and applied impact(see detailed results). Among the theoretical results we underline those presented in conferences like Principles of programming languages POPL 2016, and among the applied results we underline the release of MemCad, the first analyzer that can handle the analysis of various data structures.

# CELTIQUE Project-Team (section vide)

# DEDUCTEAM Team (section vide)

**GALLIUM Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Xavier Leroy received the 2016 Royal Society Milner Award "in recognition of his exceptional achievements in computer programming which includes the design and implementation of the OCaml programming language".

Xavier Leroy received one of the two 2016 Van Wijngaarden Awards from Centrum Wiskunde & Informatica (Amsterdam).

Xavier Leroy received the ACM SIGPLAN Most Influential POPL Paper Award for his POPL 2006 paper, *Formal certification of a compiler back-end or: programming a compiler with a proof assistant* [51].

# MARELLE Project-Team (section vide)

**MEXICO Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### Diagnosis, Anti-alignments and Coverability

DIAGNOSIS

Several new advances were obtained, concerning Diagnosis in Infinite-State Probabilistic Systems, Approximate Diagnosability of Stochastic Systems, and Diagnosability of Repairable Faults; see the 'New Results' section for a detailed description.

ANTI-ALIGNMENTS IN CONFORMANCE CHECKING – THE DARK SIDE OF PROCESS MODELS

Conformance checking techniques asses the suitability of a process model in representing an underlying process, observed through a collection of real executions. These techniques suffer from the well-known state space explosion problem, hence handling process models exhibiting large or even infinite state spaces remains a challenge. One important metric in conformance checking is to asses the precision of the model with respect to the observed executions, i.e., characterize the ability of the model to produce behavior unrelated to the one observed. By avoiding the computation of the full state space of a model, current techniques only provide estimations of the precision metric, which in some situations tend to be very optimistic, thus hiding real problems a process model may have. In [15], [25] we present the notion of anti-alignment as a concept to help unveiling traces in the model that may deviate significantly from the observed behavior. Using anti-alignments, current estimations can be improved, e.g., in precision checking. We show how to express the problem of finding anti-alignments as the satisfiability of a Boolean formula, and provide a tool which can deal with large models efficiently. In [19], [20], a novel approach to measure precision and generalization is presented, which relies on the notion of anti-alignments. We propose metrics for precision and generalization that resemble the leave-one-out cross-validation techniques, where individual traces of the log are removed and the computed anti-alignment assess the model's capability to describe precisely or generalize the observed behavior.

APPROACHING THE COVERABILITY PROBLEM CONTINUOUSLY

The coverability problem for Petri nets plays a central role in the verification of concurrent shared-memory programs. However, its high EXPSPACE-complete complexity poses a challenge when encountered in real-world instances. In [13], we develop a new approach to this problem which is primarily based on applying forward coverability in continuous Petri nets as a pruning criterion inside a backward coverability framework. A cornerstone of our approach is the efficient encoding of a recently developed polynomial-time algorithm for reachability in continuous Petri nets into SMT. We demonstrate the effectiveness of our approach on standard benchmarks from the literature, which shows that our approach decides significantly more instances than any existing tool and is in addition often much faster, in particular on large instances.

**PARSIFAL Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

D. Miller gave invited talks at the following two regularly held international meetings.

- TYPES 2016: 22nd International Conference on Types for Proofs and Programs (Novi Sad, Serbia, 23-26 May 2016) and
- Linearity 2016: 4th International Workshop on Linearity (Porto, 25 June 2016).

D. Miller gave invited talks at the following research oriented meetings.

- Workshop on linear logic, mathematics and computer science as part of "LL2016-Linear Logic: interaction, proofs and computation", 7-10 November 2016, Lyon. France.
- Research seminar titled "Interactions between logic, computer science and linguistics: history and philosophy", Université de Lille 3, 15 June 2016.
- CIPPMI (Current issues in the philosophy of practice of mathematics and informatics) Workshop on Proofs, justifications and certificates. 3-4 June 2016, Toulouse, France.

A seminar in honor of the 60th birthday of Professor Miller was held on 15-16 December at Université Paris Diderot-Paris 7 in Paris, France. Several members of the team contributed talks and original research papers.

- Tomer Libal and Marco Volpe, *A general proof certification framework for modal logic*.
- Roberto Blanco and Zakaria Chihani, *An interactive assistant for the definition of proof certificates*. Preprint available as [36].
- Lutz Straßburger, *Combinatorial flows as proof certificates with built-in proof compression*.
- Taus Brock-Nannestad, *Substructural cut elimination*.

B. Accattoli gave an invited talk at the following regularly held international meeting.

- WPTE 2016: 3rd International Workshop on Rewriting Techniques for Program Transformations and Evaluation (Porto, 23 June 2016).

S. Graham-Lengrand gave an invited talk at the following international conference.

- CLAM 2016: 5th Latin American Congress of Mathematicians, thematic session on Logic and Computability (Barranquilla, Colombia, 15th July 2016).

# PI.R2 Project-Team (section vide)

**SUMO Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

**Start-up creation**. Christophe Morvan (Ass. Prof. Univ. Paris Est Marne la Vallée) has been hosted by Sumo for several years for his research activities. In 2016, he created Open Agora with two other computer scientists. The company develops a software suite to help the decision process in large structures. It offers tools to structure discussions, voting mechanisms, and automated argument summaries. The company will maintain connections with the team for the development of GAGs (Guarded Attributed Grammars) that are instrumental in the automated summary tools.

**New team member**. Nicolas Markey (DR CNRS) recently joined the team, after several years in LSV (*Laboratoire Spécification et Vérification*), Cachan. Nicolas will reinforce the activities of the team in the modeling and analysis of timed systems, abstraction techniques and game theory.

**TOCCATA Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

- S. Conchon: co-organizes POPL'2017 (January, Paris, http://conf.researchr.org/home/POPL-2017)
  - Major Int. Conference on Foundations of Programming Language, Semantics, Type Systems, Formal Proof Techniques

### *5.1.1. Awards*

- [April 2016] Martin Clochard, Léon Gondelman, Mário Pereira: jointly receive the "Best student team" award of the *VerifyThis@ETAPS2016 verification competition*
- [July 2016] S. Boldo: Best Talk Award at workshop NSV *Computing a correct and tight rounding error bound using rounding-to-nearest*

**VERIDIS Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Jasmin Blanchette was awarded an ERC Starting Grant for his Matryoshka project aiming at fast interactive verification through strong automation for higher-order constructs.

As part of a European network, Pascal Fontaine and Thomas Sturm participate in a new H2020 Coordination and Support Action. [0] In accordance with the distributed character of Veridis, we are operating nodes at LORIA as well as MPI. Further nodes are located in Austria (University of Linz), Germany (RWTH Aachen; University of Kassel), Italy (Fondazione Bruno Kessler; University of Genova), and the UK (Universties of Bath, Coventry, and Oxford; Maplesoft Europe Ltd.). The CSA aims at improving the integration of communities, methods, and software from SMT solving and symbolic computation [20].

Jasmin Blanchette and Stephan Merz were PC chairs and organizers of the 7th International Conference on Interactive Theorem Proving in Nancy (August 22–27), the main conference of developers and users of proof assistants.

### *5.1.1. Awards*

Mathias Fleury, together with his two supervisors, received the Best Paper Award at IJCAR 2016 for their work on a formalized SAT solver.

Together with Andrew J. Reynolds at the University of Iowa, Jasmin Blanchette was invited to submit a short version of his CADE 2015 paper on a decision procedure for (co)datatypes to the Sister Conference Best Paper Track of IJCAI 2016.

BEST PAPERS AWARDS :

[25] **8th International Joint Conference on Automated Reasoning (IJCAR 2016)**. J. C. BLANCHETTE, M. FLEURY, C. WEIDENBACH.

[19] **IJCAI 2016**. A. REYNOLDS, J. C. BLANCHETTE.

[0] H2020-FETOPEN-2015-CSA-712689, http://www.sc-square.org/

**CARTE Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

The Marie Curie RISE project *Computing with Infinite Data* coordinated by Dieter Spreen (Siegen University), in which Mathieu Hoyrup is participating, has been accepted. It will start in April 2017.

**COMETE Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### *5.1.1. Notable New Projects and Contracts*

- New ANR project REPAS: Reliable and Privacy-Aware Software Systems via Bisimulation Metrics (Section 9.3.4.1 )
- New industrial contract with Renault: Protection techniques for location data (Section 8.1.1 )

# DICE Team (section vide)

**PESTO Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

Steve Kremer gave a keynote talk at the 29th IEEE Computer Security Foundations Symposium (CSF'16).

### *5.1.1. Awards*

Véronique Cortier, Antoine Dallon and Stéphanie Delaune received the EASST best paper award of the ETAPS conference for the paper [24].

BEST PAPERS AWARDS :

[24] **5th International Conference on Principles of Security and Trust (POST'16)**. V. CORTIER, A. DALLON, S. DELAUNE.

**PRIVATICS Project-Team**

# 4. Highlights of the Year

## 4.1. Highlights of the Year

In 2014, Jagdish Prasad Achara, Mathieu Cunche and Vincent Roca published with Aurelien Francillon from Eurecom a study on the Wi-Fi permissions used by mobile applications and their privacy implications. Two years after our research was published, the Federal Trade Commission (FTC) reached a $950,000 settlement with InMobi for tracking millions of consumers' locations, including children, without their knowledge. The FTC allege that InMobi abused the WiFi State information on the Android system to track the location of people without their consent, which is exactly what we showed in our research. Its policy prevents the FTC of releasing the sources of its investigations, therefore there is no way to affirm that our research triggered this investigation or was used during this investigation. We can only be sure that we identified a privacy issue that was serious enough to justify an investigation of the FTC and a penalty of $950,000. In addition to this, the company is under surveillance for their privacy behaviour for the next 20 years.

### *4.1.1. Awards*

The software `MyTrackingChoices` designed by Claude Castellucia and Jagdish Prasad Achara from Privatics in collaboration with Javier Parra (former member of Privatics and now at Universitat Politecnica de Catalunya) was awarded 'Data protection by design' award by the Catalan Data Protection Authority.

**PROSECCO Project-Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

This year, we published 18 articles in international peer-reviewed journals and conferences, including papers in prestigious conferences such as POPL, IEEE S&P Oakland, ACM CCS, NDSS, CSF, and WPES. Notably, Bruno Blanchet published a book surveying the use of ProVerif, his state-of-the-art protocol verification tool. We also won several research awards for our work, detailed below. Our work also exposed two new attacks, SLOTH and SWEET32, on Transport Layer Security, resulting in security updates and CVEs in popular web browsers and VPN software.

### *5.1.1. Awards*

- Catalin Hritcu was awarded an ERC Starting Grant
- Catalin Hritcu was awarded an ANR Jeune Chercheur/Jeune Chercheuse Grant
- Karthikeyan Bhargavan was awarded an ERC Consolidator Grant
- Karthikeyan Bhargavan and Gaëtan Leurent won a Best Paper award at NDSS 2016
- Karthikeyan Bhargavan, Cedric Fournet, Markulf Kohlweiss, and Alfredo Pironti were awarded the Levchin prize for contributions to Real-World Cryptography
- Karthikeyan Bhargavan was awarded a Microsoft Outstanding Collaborator Award
- Karthikeyan Bhargavan was awarded the Prix Inria – Académie des sciences du Jeune chercheur

**TAMIS Team**

# 5. Highlights of the Year

## 5.1. Highlights of the Year

### New major release of Plasma Lab

**Participants:** Axel Legay, Sean Sedwards, Louis-Marie Traonouez.

We have released version 1.4.0 of our Plasma Lab software. This new version introduces a new command line interface for launching Plasma Lab. Besides the Graphical Interface, most of Plasma Lab functionalities are now available directly from the command line. Additionally the new version includes a new algorithm for cross entropy minimization using importance sampling. It allows to estimate the probabilities of rare events.

### Fault injection proof-of-concept

**Participants:** Axel Legay, Jean-Louis Lanet, Thomas Given-Wilson, Nisrine Jafri.

Creation of a proof of concept to show that formal verification can be used to discover fault injections induced by hardware attacks.

### Creation of LHS platform

**Participants:** Jean-Louis Lanet, Hélène Le Bouder, Ronan Lashermes.

Entry into service of the LHS platform that can be used to monitor systems, inject faults, or reason on ransomware.

### Taler Systems startup creation

**Participants:** Jeffrey Burdges, Florian Dold, Christian Grothoff, Marcello Stanisci.

A startup, Taler Systems S.A. was formally created, and we started the contractual paperwork required. An interview was given to RWGV-Genossenschaftsblatt (an internal publication of a large group of German banks).

### Contract with CISCO

**Participants:** Axel Legay, Fabrizio Biondi, Thomas Given-Wilson.

Signature of a major research collaboration contract between Tamis and CISCO to work on malware analysis. The collaboration will fund 3 engineers, trips to visit CISCO and participate to conferences on the topic, as well as a powerful servers to store and analyse malware.

### Awards

Axel Legay received the first Parnass award.

Christian Grothoff became an Ashoka fellow.