RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2015

Section Highlights of the Team

Edition: 2016-03-21

Algorithmics, Computer Algebra and Cryptology

Architecture, Languages and Compilation

Embedded and Real-time Systems

Proofs and Verification

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. ARITH conference in Lyon

Since 1969, ARITH is the primary and reference international conference for presenting scientific work on the latest research in computer arithmetic. In June 2015, we organized it in Lyon.

5.1.2. Best student paper

At ISSAC'2015 [20].

5.1.3. Best papers

Best papers at Eurocrypt'2015 , Asiacrypt'2015 and ISSAC'2015 .
BEST PAPERS AWARDS :
[14] **EUROCRYPT**. J. H. CHEON, K. HAN, C. LEE, H. RYU, D. STEHLÉ.
[11] **ASIACRYPT**. S. BAI, A. LANGLOIS, T. LEPOINT, D. STEHLÉ, R. STEINFELD.
[16] **ISSAC**. J.-G. DUMAS, C. PERNET, Z. SULTAN.

CARAMEL Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

The LOGJAM attack has received the best paper award at the conference ACM CCS 2015 (Conference on Computer and Communications Security). It has also received a Pwnie award [0] in the category *Most innovative research*.

The Tower NFS article was one of the two ASIACRYPT 2015 papers invited to submit a long version to Journal of Cryptology.

BEST PAPERS AWARDS :

[15] **ACM CCS 2015**. D. ADRIAN, K. BHARGAVAN, Z. DURUMERIC, P. GAUDRY, M. GREEN, J. A. HALDERMAN, N. HENINGER, D. SPRINGALL, E. THOMÉ, L. VALENTA, B. VANDERSLOOT, E. WUSTROW, S. ZANELLA-BÉGUELIN, P. ZIMMERMANN.

[17] **ASIACRYPT 2015**. R. BARBULESCU, P. GAUDRY, T. KLEINJUNG.

[0] http://pwnies.com/

CASCADE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Conferences

Our group presented 8 papers (among 57) at Eurocrypt, 7 (among 74) at Crypto, and 3 (among 64) at Asiacrypt, the main general IACR conferences, and 6 papers (among 36) at PKC and 2 (among 34) at CHES, the two thematic IACR conferences on our domains (public-key cryptography and hardware-oriented cryptography).

5.1.2. Awards

In February 2015, Tancrède Lepoint has received the Gilles Kahn PhD Thesis Award 2014.

CRYPT Team

4. Highlights of the Year

4.1. Highlights of the Year

In [16], the team introduced a new method to construct truncated differential characteristics of block ciphers: truncated differential cryptanalysis is a popular generalization of differential cryptanalysis. Using this method, the team has found improved attacks on the block ciphers CLEFIA and Camellia, which are both standardized by ISO.

GALAAD2 Team (section vide)

GEOMETRICA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Clément Maria has been awarded the Prix de thèse Gilles Kahn - Académie des Sciences.

5.1.2. Books

Steve Oudot published a book on persistence theory in the AMS series *Mathematical Surveys and Monographs* [35].

GRACE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Freestart collision for the full SHA-1.

Together with M. Stevens and T. Peyrin, P. Karpman gave the first freestart collision for the full SHA-1 hash function [32]. Although theoretical attacks on this function were known since 2005, this work is an important milestone in SHA-1 cryptanalysis and it had a concrete impact on the use of SHA-1 in existing systems, such as TLS certificates. In particular, the CA/Browser forum (which regroups some of the major industries of the internet) withdrew an internal ballot proposing to extend the use of SHA-1 in new certificates through 2016. Major browser developers such as Mozilla are also encouraging the timely withdrawal of SHA-1 certificates by updating the in-browser security warnings when such certificates are used. This result was also vulgarised in technical press such as *Ars Technica* and more general newspapers such as *Le monde*.

Discrete logarithm record computation in finite fields

F. Morain and A. Guillevic together with P. Gaudry (CARAMEL team, Inria Nancy Grand Est) and R. Barbulescu (CNRS, IMJ) published a new discrete logarithm record in a finite field of 180 decimal digits (dd), i.e. 595 bits. This result was presented at the Eurocrypt 2015 conference [19]. The Discrete Logarithm Problem (DLP) is widely studied in prime fields GF(p) and was broken in small characteristic finite fields of the form GF(2^n) and GF(3^n) with smooth n very recently. It was not known whether the DLP is as hard in extensions of finite fields compared to prime fields, for the same global size. With this record of the same size as the most recent record in a prime field, F. Morain and A. Guillevic showed that DLP in GF(p^2) is much faster than in a prime field of the same size, and even faster than a factorization of an RSA modulus of the same size.

Table 1. Comparison of running time for integer factorization (NFS-IF), discrete logarithm in prime field (NFS-DL(p)) and in quadratic field (NFS-DL(p 2)) of same global size 180 dd.

Algorithm	relation collection	linear algebra	total
NFS-IF	5 years	5.5 months	5.5 years
NFS-DL(p)	50 years	80 years	130 years
NFS-DL(p^2)	157 days	18 days (GPU)	0.5 years

F. Morain and A. Guillevic contributed with P. Gaudry and E. Thomé to other DL computation records in finite fields GF(p^3) of 508 bits and 512 bits, and GF(p^4) of 392 bits. The practical difficulty is increasing with the extension degree.

CATREL conference

The 1st and 2nd of October 2015, F. Morain, B. Smith and A. Guillevic organized an international workshop to conclude the CATREL project. There were 14 invited speakers from all around the world, from Palaiseau with A. Guillevic to as far as Auckland in New Zealand with S. Galbraith. A. Joux presented an historical summary of DL computation from the 80's. P. Gaudry, E. Thomé and C. Bouvier from the Caramel Team (Inria Nancy), presented their contribution, and K. Bhargavan presented the Logjam attack. There were also members of abroad teams leader in discrete logarithm record breaking. G. Adj from Mexico and R. Granger and T. Kleinjung presented their recent records in small characteristic.

We hosted more than 50 participants for the two intensive days of the workshop. The schedule of the workshop is available on the following link. http://www.lix.polytechnique.fr/cryptologie/CATREL-workshop

AGC^{2}T 15

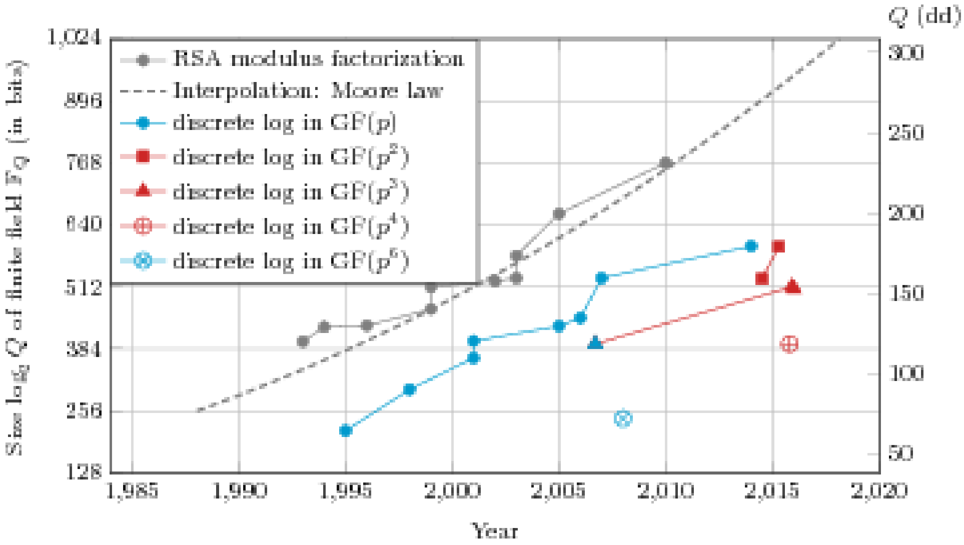

Figure 1. Records of DL computation in finite fields, and RSA modulus factorization. F. Morain and A. Guillevic contributed to the records in red in 2014–2015.

A. Couvreur was one of the organizers of the conference AGC^{2}T 15 (Arithmetic Geometry Cryptography and Coding Theory) at CIRM (Marseille).

LFANT Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

The team has been evaluated in 2015, and our scientific project for the next four years has been validated by the external reviewers.

Fredrik Johansson, who was already a postdoc last year, has been recruited as a full time researcher.

The team has organised the Atelier Pari/GP in January 2015 and the ECC 2015 international conference (with a summer school) in September 2015.

Athanasios Angelakis has defended his PhD thesis on *Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves* in September 2015.

Julio Brau has defended his PhD thesis on *Galois representations of elliptic curves and abelian entanglements* in December 2015.

Enea Milio has defended his PhD thesis on *Computing modular polynomials in dimension 2* [11] in December 2015.

The European H2020 project OpenDreamKit, in which the team participates, has been accepted.

POLSYS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Our joint research project GOAL@SiliconValley with Californian University UC Berkeley has been selected by Inria (2015-2018). GOAL led by Bernd Sturmfels (UC Berkeley) and Jean-Charles Faugère (POLSYS, Inria Paris-Rocquencourt) on “Geometry and Optimization with ALgebraic methods“: The goal of this project is to develop algorithms and mathematical tools to solve geometric and optimization problems through algebraic techniques. As a long-term goal, the joint team plans to develop new software to solve these problems more efficiently. These objectives encompass the challenge of identifying instances of these problems that can be solved in polynomial time with respect to the number of solutions and modeling these problems with polynomial equations.

The webpage of the research project is http://www-polsys.lip6.fr/GOAL/index.html

The kickoff workshop was held at UC Berkeley in May 2015, see https://math.berkeley.edu/~bernd/GOALworkshop.html.

SECRET Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Resistance of equivalent Sboxes to differential and linear attacks

The so-called Sboxes highly influence the security of a block cipher since they are the only nonlinear component in the cipher. It was widely believed that Sboxes which are affine equivalent (i.e., which are the same up to the composition with affine functions) provide the same security level regarding differential and linear cryptanalyses. However, some simulation results on the maximum expected differential probability over two rounds of the AES show that this is not always the case. A. Canteaut and J. Roué [45] have then investigated the effect of affine transformations of the Sbox on the maximal expected differential probability and linear potential over two rounds of a substitution-permutation network, when the diffusion layer is linear over the finite field defined by the Sbox alphabet. They have been able to exhibit different behaviors depending on the choice of the Sbox within a given equivalence class. This includes some unexpected differences: for a given m-bit Sbox, the choice of the basis used for defining the finite field in the description of the linear layer may also affect the value of the two-round MEDP or MELP. They have also shown that the inversion is the mapping within its equivalence class which has the highest two-round MEDP and MELP, independently of the choice of the MDS linear layer. This situation mainly originates from the fact that this Sbox is an involution. This result has been awarded as one of the 3 best papers at Eurocrypt 2015.

5.1.2. Relativistic cryptography

Two-party cryptographic tasks are well-known to be impossible without complexity assumptions, either in the classical or the quantum world. Remarkably, such no-go theorems might become invalid when adding the physical assumption that no information can travel faster than the speed of light. This additional assumption gives rise to the emerging field of relativistic cryptography. We started investigating such questions through the task of bit commitment. In particular, an interesting bit commitment protocol was introduced in 2014 by Lunghi *et al.* and proven secure against arbitrary classical attacks. The drawback however was that the commitment time was quite constrained, as most a few milliseconds. In [16], K. Chakraborty, A. Chailloux and A. Leverrier showed that the same protocol could in fact achieve commitment times that were arbitrarily long, thereby establishing that relativistic cryptography is a very practical solution.

5.1.3. Quantum Expander Codes

In a paper presented at FOCS 2015 [55], A. Leverrier and JP. Tillich, together with G. Zémor, give an efficient decoding algorithm for a certain kind of quantum LDPC codes which provably corrects any pattern of errors of weight proportional to the square-root of the length of the code. The algorithm runs in time linear in the number of qubits, which makes its performance the strongest to date for linear-time decoding of quantum codes. This work can be considered as a further step towards proving that fault tolerant quantum computing is possible by using only a constant multiplicative overhead of additional qubits.

5.1.4. Organization of WCC 2015

The whole project-team has been involved in the organization of the international conference WCC 2015, which was held in Paris (at Institut Henri Poincaré) in April 2015. This was the ninth in the series of biannual workshops on *Coding and Cryptography*. This edition has gathered around 150 participants from many different countries. We received 90 submissions out of which 53 have been selected for presentation at the conference.

5.1.5. Awards

- 1st prize of the Streebog competition [90]
- 2nd prize of the underhanded crypto contest https://underhandedcrypto.com/archive/
- One of the best 3 papers at Eurocrypt 2015 [45]
- Best paper at PQCrypto 2016 [57].

BEST PAPERS AWARDS :

[45] **Advances in Cryptology - Eurocrypt 2015 (Part I)**. A. CANTEAUT, J. ROUÉ.

SPECFUN Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Pierre Lairez has been awarded this year the “Ecole Polytechnique thesis prize”, for his PhD thesis defended in 2014 [53].

VEGAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

In the context of drawing plane algebraic curves with the correct topology, we have obtained and submitted this year major results on the resolution of bivariate algebraic systems. In particular, we presented algorithms whose worst-case and expected (Las Vegas) complexities are not likely to be easily improved as such improvments would essentially require to improve bounds on other fundamental problems (such as computing resultants, checking the squarefreeness of univariate polynomials, and isolating their roots) that have hold for decades. See section 6.3.1 for details.

ALF Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Pierre Michaud won the 2nd Data Prefetching Championship held in conjunction with ISCA 2015 (Portland, June 2015).

BEST PAPERS AWARDS :

[27] **2nd Data Prefetching Championship**. P. MICHAUD.

ATEAMS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Prof.dr. Paul Klint won the IEEE TCSE Software Engineering Distinguished Service Award 2015. This award is presented "annually for outstanding and/or sustained contributions and service to the software engineering community".

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 IEEE/ACM Design Automation and Test in Europe (DATE'15) [70].

Some Granit out of Cairn... The GRANIT team at IRISA is a spin-off of the CAIRN team created in January 2015, and all of the GRANIT members were formerly belonging to CAIRN. This decision was motivated by two main reasons: CAIRN had reached a critical size (nearly twenty permanent researchers) and the scope of its research was becoming really broad. During the last period, the global scope of CAIRN was the research of new architectures, algorithms and design methods for flexible and energy efficiency domain-specific system-on-chip (SoC), promoting the use of reconfigurable hardware. The research activities of CAIRN were organized around three main topics: (i) The invention and the design of new reconfigurable platforms with an emphasis on flexible arithmetic operator design, dynamic reconfiguration management and low-power consumption. (ii) The development of their corresponding design flows (compilation and synthesis tools) to enable their automatic design from high-level specifications. (iii) The interaction between algorithms and architectures especially for wireless communications and wireless sensor networks. In brief, the two first topics will still be investigated by CAIRN, while GRANIT will explore the third one, with a new focus on algorithm and architecture adaptivity and cooperation between wireless nodes.

Awards The paper "Energy-Aware Computing via Adaptive Precision under Performance Constraints in OFDM Wireless Receivers" [39] received the best paper at the IEEE Computer Society Annual Symposium on VLSI (ISVLSI).

BEST PAPER AWARD :

[39] **IEEE Computer Society Annual Symposium on VLSI (ISVLSI 15)**. F. CLADERA, M. GAUTIER, O. SENTIEYS.

CAMUS Team

5. Highlights of the Year

5.1. Highlights of the Year

Aravind Sukumaran-Rajam has shown in his PhD work [13] that the polyhedral model, usually exclusively dedicated to advanced static analysis and optimization of linear loops, can also be applied to nonlinear loops. This noteworthy extension of the scope of polyhedral techniques has been made possible thanks to the speculative and dynamic parallelization strategy implemented in the Apollo framework. Significant parallel speed-ups can now be obtained automatically for loops and loop nest that could not be handled before by compilers. Aravind Sukumaran-Rajam and Philippe Clauss have published a paper on this topic in the ACM journal Transactions on Architecture and Code Optimization in 2015 [14].

COMPSYS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Scientific Results

2015 showed good successes, in terms of scientific results, with respect to the objectives we fixed for Compsys III, i.e., pushing static compilation beyond its present limits, both in terms of techniques and applications, bridging the gap between polyhedral techniques and abstract interpretation, sequential codes and parallel specifications, back-end and front-end techniques. Important advances in 2015 are as follows:

- **Towards a polynomial model** We developed new techniques to handle polynomials (see Section 7.11) and thereby generalizing polyhedral (e.g., affine) techniques, with applications to the analysis of the OpenStream parallel language (see Section 7.10).
- **Handling parallel specifications** In complement to our current studies of parallel languages such as X10 (see Sections 7.8 and 7.9) and OpenStream (see Section 7.10), and kernel offloading with pipelined specifications (see Section 7.7), we succeeded to extend liveness analysis (see Section 7.12) and array contraction (see Section 7.13) to parallel specifications.
- **Enhancing interactions between programmer and compiler** This is an important challenge for the expansion of the applicability of our techniques. The work exposed in Sections 7.9 and 7.15 (effort for collecting and analyzing real applications), as well as the interaction with users of HPC, including the organization a joint spring school in 2016, are important steps in this direction.
- **Links with abstract interpretation and SMT solvers** The extension of our previous work on loop termination, with an iterative technique relying on SMT solvers for exhibiting counter-examples (see Section 7.4), is an interesting combination of polyhedral and abstract interpretation techniques. This is the case also for the array analysis of Section 7.3 .
- **Back-end analysis** Considering back-end optimizations remains important, as complementary to front-end optimizations. See the results on register spilling (Section 7.1), pointer analysis (Section 7.2), liveness analysis (Section 7.12), the latter exploiting the fact that a polyhedral representation of arrays and loops is a symbolic unrolled view of registers and traces.

Awards

The CC'15 paper on parametric tiling [3] was nominated as a best paper candidate for the group of conferences ETAPS'15 where, unfortunately, CC papers never finally got an award.

End of Compsys

Compsys exists since 2012 as an Inria team. It has been created in 2004 as an Inria project-team, and evaluated by Inria first in 2007, then in 2012. It will again be evaluated in March 2016, which will be its final evaluation as an Inria project-team is limited to 12 years. The construction of a new project is thus necessary. The research directions of Compsys III were already a shift towards this future project. A few tentative research directions may be:

- 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 makes it difficult to have a clear view of the future.

CORSE Team (section vide)

DREAMPAL Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

2015 has been a good year in terms of journal publications for Dreampal, with 8 articles mostly in very high-quality venues.

POSTALE Team

4. Highlights of the Year

4.1. Highlights of the Year

Marc Baboulin was invited plenary speaker at the HPCSE conference, Solan, Czech Republic, May 25-28, 2015.

The Random Butterfly Transformations developed by Postale are now available in the MAGMA library for GPU (release 1.6) and Intel Xeon Phi (release 1.3).

Marc Baboulin is general vice-chair of the HPC Symposium to be held in April 2016, Pasadena, CA.

TASC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

1. The PhD thesis of Jean-Guillaume Fages about *the use of graph structure in constraint programming* got the following awards:
   - PhD thesis award by the French association for AI.
   - Doctoral research award by the Association for Constraint Programming.
2. The paper of the PhD student Anicet Bart (*Verifying a Real-Time Language with Constraints*, Anicet Bart, Charlotte Truchet and Eric Monfroy [29]) got the best paper award of the SAT/CSP track of the ICTAI 2015 conference.
3. The solver Choco3 got a bronze medal in the 2015 minizinc challenge.

BEST PAPERS AWARDS :

[29] **27th IEEE International Conference on Tools with Artificial Intelligence**. A. BART, C. TRUCHET, E. MONFROY.

AOSTE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Robert Davis, from York University, got awarded an Inria International Chair to spend a year over a duration of five years as full member of the Aoste EPI.

CONVECS Project-Team (section vide)

HYCOMES Team

4. Highlights of the Year

4.1. Highlights of the Year

The main progress on hybrid systems modeling can be summarized as follows:

- As part of his PhD work, Ayman Aljarbouh has designed and implemented regularization techniques for hybrid systems with chattering behaviour [9]. His techniques enable the efficient simulation of chattering behavior that can not be simulated with pure *event-driven* simulation techniques.
- A constructive semantics for guarded DAE systems has been proposed. Guarded DAE systems are equivalent to the kernel language used as an intermediate format by several Modelica compilers. This semantics, based on a nonstandard (infinitesimal) time model [3], allows to determine the structural differentiation index and infer the causal dependencies of a system of guarded DAEs. The semantics has been implemented in SUNDAE, a prototype software, developed in the context of the Sys2soft (7.2) and Modrio projects (7.3.1).

MUTANT Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Best Student Paper Award, *IEEE 2015 International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, in *Machine Learning for Signal Processing Category*

Best Student Paper award, *International Symposium on Computer Music Interdisciplinary Research 2015 (CMMR)*

Public Antescofo Open Mic Session, Ircam Open House on June 2015 (with 2000+ participants).

Numerous Public Concerts worldwide including performances with (2015 highlights) *Berlin Philharmonics* (March), *Barbican Center in London* (May), *Warsaw Autumn Festival*, and more.
BEST PAPERS AWARDS :
[11] **ICASSP 2015 - 40th IEEE International Conference on Acoustics, Speech and Signal Processing**. A. BIETTI, F. BACH, A. CONT.
[22] **International Symposium on Computer Music Multidisciplinary Research (CMMR)**. I. YUPING REN, R. DOURSAT, J.-L. GIAVITTO.

PARKAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Awards

Albert Cohen received a HiPEAC Industry Transfer Award for the Polly Labs initiative, in collaboration with Sven Verdoolaege, Tobias Grosser (now ETH Zürich), and ARM. The award comes with a 1000 euro gift.

Louis Mandel and Marc Pouzet received the price for the “Most influential PPDP’05 paper “ReactiveML: a reactive extension to ML” given at the PPDP conference, in Siena (Italy), in July 2015.

POSET Team

5. Highlights of the Year

5.1. Highlights of the Year

Two presentations, by D. Janin and S. Salvati, at ICALP 2013, a leading conference in the field of formal language theory and its applications to computer science, have eventually been selected among the 16 out of 120 papers for a complete version to appear this year in the associated special issue (see [15] and [16]).

SPADES Project-Team (section vide)

TEA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

TEA became an Inria project-team in 2015 and developed new and promising collaborations with Mitsubishi, on factory automations, with UCSD on refinement type theory and with UCSD-UCLA again, on time synchronisation protocols verificaton.

We published a paper in the automotive session of the 52nd. Digital Automation Conference (core A*) on our project with Toyota ITC [19] as well as two patents filed with the USPTO.

5.1.1. Awards

Our paper on "Polychronous automata" [13] received the Best Paper Award at the TASE'15 conference.
BEST PAPERS AWARDS :
[13] **TASE 2015, 9th International Symposium on Theoretical Aspects of Software Engineering**. P. LE GUERNIC, T. GAUTIER, J.-P. TALPIN, L. BESNARD.

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Alan Schmitt has received the 2015 Most Influential POPL Paper Award for the 2005 paper “Combinators for Bi-Directional Tree Transformations: A Linguistic Approach to the View Update Problem” [8].

DEDUCTEAM Team

5. Highlights of the Year

5.1. Highlights of the Year

Deducteam released a new version of Dedukti, more efficient, and with new features (e.g. higher-order patterns, confluence checking).

ESTASYS Team

4. Highlights of the Year

4.1. Highlights of the Year

The ESTASYS team has developped a full tool chain for the rigorous design of Systems of Systems and has achieved its two years objectives. The team has also prepared its reconfiguration into a new team where security issues will become fundamental.

4.1.1. Awards

Axel Legay has received a Villumn award from Aalborg University.

GALLIUM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

In 2015, Xavier Leroy was appointed Fellow of the ACM “for contributions to safe, high-performance functional programming languages and compilers, and to compiler verification”.

Xavier Leroy will receive the 2016 Royal Society Milner Award.

MARELLE Project-Team (section vide)

MEXICO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Major Results

5.1.1.1. 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 [39], 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.

5.1.1.2. An Automata-Theoretic Approach to the Verification of Distributed Algorithms

In [21] we introduce an automata-theoretic method for the verification of distributed algorithms running on ring networks. In a distributed algorithm, an arbitrary number of processes cooperate to achieve a common goal (e.g., elect a leader). Processes have unique identifiers (pids) from an infinite, totally ordered domain. An algorithm proceeds in synchronous rounds, each round allowing a process to perform a bounded sequence of actions such as send or receive a pid, store it in some register, and compare register contents w.r.t. the associated total order. An algorithm is supposed to be correct independently of the number of processes. To specify correctness properties, we introduce a logic that can reason about processes and pids. Referring to leader election, it may say that, at the end of an execution, each process stores the maximum pid in some dedicated register. Since the verification of distributed algorithms is undecidable, we propose an underapproximation technique, which bounds the number of rounds. This is an appealing approach, as the number of rounds needed by a distributed algorithm to conclude is often exponentially smaller than the number of processes. We provide an automata-theoretic solution, reducing model checking to emptiness for alternating two-way automata on words. Overall, we show that round-bounded verification of distributed algorithms over rings is PSPACE-complete.

5.1.1.3. Unfolding-Based Process Discovery

In [33] we presents a novel technique for process discovery. In contrast to the current trend, which only considers an event log for discovering a process model, we assume two additional inputs: an independence relation on the set of logged activities, and a collection of negative traces. After deriving an intermediate net unfolding from them, we perform a controlled folding giving rise to a Petri net which contains both the input log and all independence-equivalent traces arising from it. Remarkably, the derived Petri net cannot execute any trace from the negative collection. The entire chain of transformations is fully automated. A tool has been developed and experimental results are provided.

PARSIFAL Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Accattoli's paper with Ugo Dal Lago titled "Beta Reduction is Invariant, Indeed" that appeared in CSL-LICS 2014 was invited to a special issue of LMCS of selected papers from that meeting.

Miller ended his second and final term as the Editor-in-Chief of the ACM Transactions on Computational Logic. He remains as an Area Editor for Proof Theory.

Miller was a plenary speaker at the joint meeting of LOPSTR 2015 and PPDP 2015 (Siena, Italy) and was an invited speaker at LSFA 2015 (Natal Brazil) and in the Session on History and Philosophy of Computing at the 15th Congress of Logic, Methodology and Philosophy of Science, Helsinki.

Miller spoke at the ETH Zurich Department of Computer Science Distinguished Colloquium Series on April 20.

Graham-Lengrand gave an invited talk at the IFIP Working Group 1.6 on Term Rewriting, on the occasion of its 2015 annual meeting in Warsaw, Poland.

Accattoli was an invited speaker at the 16th International Workshop on Logic and Computational Complexity (Kyoto, Japan, 5th of July).

PI.R2 Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Coq 8.5

Version 8.5 of Coq will remain as one of the most important versions of the history of Coq. It includes five big achievements affecting various components of the system: a new proof engine supporting multi-goal and deep backtracking by Arnaud Spiwack; a new asynchronous evaluation engine supporting efficient parallel development of interactive documents, parallel evaluation of tactics, modular compilation of files by Enrico Tassi; full universe polymorphism by Matthieu Sozeau; a new notion of primitive projections highlighting the negatively polarised view at record types by Matthieu Sozeau; a new evaluation machine by Maxime Dénès which works by compiling to OCaml.

The year 2015 was also a year of thinking on new ways to popularise Coq and further enhance the interaction between users and developers. In particular, a first Coq Coding Sprint gathered about 30 participants around about 10 developers.

4.1.2. EPIT 2015

This year, the French Spring School in Theoretical Computer Science (EPIT) was organised by Yann Régis-Gianas, Pierre Letouzey, Matthieu Sozeau and Pierre-Marie Pédrot in Fréjus (France). This CNRS “école thématique” was dedicated to the mechanisation of proofs of programs and of mathematical theorems in Coq. It was attended by 50 participants, coming from different research communities. Besides the courses introducing the basics of Coq and proof development in Coq, substantial efforts of formalisation in various areas such as formal language theory, number theory, or combinatorics were presented by their authors, and the attendants were encouraged to discuss their own formalisation projects with the Coq developers. The school has been sponsorised by the CNRS, the FIFP, the ADT Coq and the ANR Paral-ITP. The feedback from the participants was very positive.

SUMO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The book on "Petri Net Synthesis" [44] co-authored by Eric Badouel, Luca Bernardinello, and Philippe Darondeau was published in October 2015 by Springer-Verlag in the EATCS Series "Texts in Theoretical Computer Science". This book is a comprehensive, systematic survey of the synthesis problem, and of region theory which underlies its solution, covering the related theory, algorithms, and applications. It is also a tribute to Philippe who passed away two years ago and could not see the final result of this project.

The SUMO team also welcomes the arrival of Ocan Sankur as a CNRS researcher. After a PhD at LSV (ENS Cachan) in 2013 supervised by Patricia Bouyer and Nicolas Markey, Ocan Sankur did a post-doc at Université Libre de Bruxelles in the group of Jean-François Raskin. His research work focuses on the robustness of quantitative systems, for their verification and synthesis.

TOCCATA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- C. Paulin-Mohring received the award “Michel Monpetit – Institut National de Recherche en Informatique et en Automatique” of the French Academy of Sciences (http://www.academie-sciences.fr/fr/Laureats/laureats-2015-prix-thematiques.html).
- J.-C. Filliâtre and G. Melquiond received the “Best team” award of the VerifyThis@ETAPS2015 verification competition (http://verifythis2015.cost-ic0701.org/results). The Why3 tool also received the “Distinguished user-assistance tool feature” award.
- The *Concours Castor informatique* (http://castor-informatique.fr/) had an even larger success than in the previous years. In November 2015, more than 345,000 teenagers from over 2280 schools participated and solved the interactive tasks of the contest. Arthur Charguéraud and Sylvie Boldo, from the Toccata team, significantly contributed to the prepation of the tasks and to the organization of the contest.

VERIDIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Pascal Fontaine and Thomas Sturm, together with Erika Abraham (RWTH Aachen) and Dongming Wang (Beihang University, Beijing) organized the Dagstuhl Seminar 15471 in November 2015, on the subject of *Symbolic Computation and Satisfiability Checking*, bringing together two communities on subjects that are particularly relevant for our team.

Jasmin Blanchette and Christoph Weidenbach, together with Nikolaj Bjørner (Microsoft) and Viorica Sofronie-Stokkermans (University of Koblenz-Landau) organized the Dagstuhl Seminar 15381 in September 2015, on the subject of *Information from Deduction: Models and Proofs*. That seminar focused on added value of deduction tools beyond a yes/no answer, in particular certificates of (un)satisfiability.

We have made considerable progresses with the symbolic analysis of reaction networks. Within this interdisciplinary project, our methods have been accepted at the leading conference in symbolic computation [33], and our results with those methods have been published in a renowned journal in the natural sciences [17].

CARTE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The paper [21] published at the International Conference on Functional Programming (ICFP 2015) has given a positive answer to an open problem, conjectured to be true for a long time: the question is to know whether inductive and coinductive data types can be added to light logic based systems without breaking the complexity of the system (i.e. staying within the class of polynomial time computable functions). This issue is analog to the issue of adding inductive and coinductive data types to system F without breaking normalization, which is known to hold for a long time. To tackle this challenging question, we have studied the problem of defining algebras and coalgebras in the Light Affine Lambda Calculus, a system characterizing the complexity class FPTIME. In this system, the principle of stratification limits the ways we can use parametric polymorphism, and in general the way we can write our programs. We have shown that while stratification poses some issues to the standard System F encodings, it still permits to encode some weak form of algebra and coalgebra. Using the algebra encoding one can define in the Light Affine Lambda Calculus the traditional inductive types. Unfortunately, the corresponding coalgebra encoding permits only a very limited form of coinductive data types. To extend this class, we have studied an extension of the Light Affine Lambda Calculus by distributive laws for the modality $\S$.

5.1.1. Awards

Hugo Férée has received the Ackermann award for his PhD thesis “complexité d’ordre supérieur et analyse récursive”.

CASSIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Véronique Cortier has obtained the prestigious Inria-French Académie des sciences Young Researcher Award.

Steve Kremer has been awarded an European Research Council (ERC) Consolidator Grant to fund his work on the specification and formal verification of new security properties.

Two junior permanent members have been hired: Vincent Cheval as CR Inria and Jannik Dreier as associate professor at Université de Lorraine.

COMETE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- SIGSAC Doctoral Dissertation Award 2015 for the thesis “Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy” [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)
- Prix de thèse de l’Ecole Polytechnique 2015 for the thesis “Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy” [29] by Nicolás Bordenabe (Defended on Sep 12, 2014)

DECENTRALISE Team (section vide)

DICE Team (section vide)

PRIVATICS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Our work on “Probabilistic k^m-anonymity” was published in the IEEE International Conference on Big Data (BigData) 2015.

Our results on Password security, “Faster Password Guessing Using an Ordered Markov Enumerator” and “Interleaving Cryptanalytic Time-memory Trade-offs on Non-Uniform Distributions”, were published at ESSOS’15 and ESORICS’15.

The team published 2 papers about his research in the newspaper “Lemonde”, 1 article in “Science & Avenir” and in “La Recherche”.

The team organized the 31 November 2015 the conference “Privacy across cultures, Convergences and divergences in a global world” in the context of the Rencontres Jacques Cartier.

4.1.1. Awards

The paper "Reasoning about privacy properties of biometric system architectures in the presence of information leakage" [15] received the best paper award at ISC 2015.
BEST PAPERS AWARDS :
[15] **Information Security Conference (ISC 2015)**. D. LE MÉTAYER, H. CHABANNE, L. ROCH, J. BRINGER.

PROSECCO Project-Team

5. Highlights of the Year

5.1. Highlights of the year

This year, we published 15 articles in international peer-reviewed journals and conferences, including papers in prestigious conferences such as IEEE S&P Oakland (2 papers), ACM CCS, NDSS, WWW, ASPLOS, and ITP, and we won four research awards for our work, detailed below.

We released updates to F*, miTLS, ProVerif, and CryptoVerif, along with our collaborators at other institutions. We discovered serious vulnerabilities in a number of TLS libraries, web browsers, and web servers, resulting in several published CVEs, and over a dozen software updates based on our recommendations in widely used software such as Firefox, Chrome, Internet Explorer, Safari, OpenSSL, Java, and Mono.

5.1.1. Awards

- Distinguished paper award, IEEE Symposium for Security and Privacy, 2015
- Best student paper award, ACM Conference on Computer and Communications Security, 2015
- Best paper award, Usenix Workshop on Offensive Technologies, 2015
- Pwnie award for Most Innovative Research, BlackHat USA, 2015