RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2012

Section highlights of the Team

Edition: 2013-04-24

ALGORITHMS, CERTIFICATION, AND CRYPTOGRAPHY
1. ARIC Team 5
2. CARAMEL Project-Team 6
3. CASCADE Project-Team (section vide) 7
4. GALAAD Project-Team (section vide) 8
5. GEOMETRICA Project-Team 9
6. GRACE Team 10
7. LFANT Project-Team 11
8. POLSYS Project-Team 12
9. SECRET Project-Team 13
10. VEGAS Project-Team 14
ARCHITECTURE AND COMPILING
11. ALF Project-Team 15
12. CAIRN Project-Team 16
13. CAMUS Team 17
14. COMPSYS Project-Team 18
EMBEDDED AND REAL TIME SYSTEMS
15. AOSTE Project-Team 19
16. CONVECS Team 20
17. DART Project-Team (section vide) 21
18. ESPRESSO Project-Team 22
19. MUTANT Project-Team 23
20. PARKAS Project-Team (section vide) 24
21. POP ART Project-Team (section vide) 25
22. S4 Project-Team (section vide) 26
23. TRIO Project-Team 27
24. VERTECS Project-Team 28
PROGRAMS, VERIFICATION AND PROOFS
25. ABSTRACTION Project-Team 29
26. ATEAMS Project-Team 30
27. CARTE Project-Team 31
28. CASSIS Project-Team 32
29. CELTIQUE Project-Team (section vide) 33
30. COMETE Project-Team 34
31. CONTRAINTES Project-Team (section vide) 35
32. DEDUCTEAM Team (section vide) 36
33. FORMES Team 37
34. GALLIUM Project-Team 38
35. MARELLE Project-Team 39
36. MEXICO Project-Team (section vide) 40
37. PAREO Project-Team 41

38. PARSIFAL Project-Team 42
39. PI.R2 Project-Team (section vide) 43
40. PROSECCO Project-Team 44
41. SECSI Project-Team 45
42. TASC Project-Team 46
43. TOCCATA Team 47
44. TYPICAL Project-Team 48
45. VERIDIS Project-Team (section vide) 49

ARIC Team

2.2. Highlights of the Year

Damien Stehlé received the CNRS-INS2I bronze medal.

2.2. Highlights of the Year

- The ANR proposal “CATREL” (in French, “Cribles, Améliorations Théoriques et Résolution Effective du Logarithme discret”) has been one of the eight accepted proposals among 59 submitted to the “programme blanc” in computer science for the year 2012. The ANR-CATREL project is beginning on January 1st, 2013.
- A new (second place) integer factorization record was set using the CADO-NFS software developed by the team, namely the factorization of RSA-704.
- Members of the team received the “Prix La Recherche” 2012 for their work on integer factorization.

CASCADE Project-Team (section vide)

GALAAD Project-Team (section vide)

GEOMETRICA Project-Team

2.2. Highlights of the Year

- Creation of a new Inria research team called TITANE on geometric modeling of 3D environments. Creation expected in 2013.
- Best Paper Award for "The Simplex Tree: An Efficient Data Structure for General Simplicial Complexes" at ESA 2012.

GRACE Team

2.1. Highlights of the Year

D. Augot co-edited a special issue of Designs, Codes and Cryptography, devoted to WCC 2011. Online versions of the articles are avalaible, while the issue will appear as volume number 66, issue 1-3, in January 2013.

LFANT Project-Team

2.2. Highlights of the Year

- Vincent Verneuil has defended his PhD thesis on “Cryptographie à base de courbes elliptiques et sécurité de composants embarqués” [12] in June 2012.
- Pierre Lezowski has defended his PhD thesis on “Questions d’Euclidianité ” [11] in December 2012.
- The ERC project ANTICS of Andreas Enge started in January 2012.
- The 2nd Atelier PARI/GP was held in 2012 (after the first installment in 2004), with the aim of creating a yearly event dedicated to the development of the main software product of the LFANT team.

POLSYS Project-Team

2.2. Highlights of the Year

- In [4], we obtain an algorithm to solve Boolean systems with an expected complexity of $O(2^{0.792\,n})$ breaking the 2^n barrier.
- In [10], we propose an algorithm to solve a variant of the Quantififer Elimination Problem for which the output formula is *almost equivalent* to the input formula. The complexity of this algorithm is much better than other algorithms and can solve previously untractable problems.
- In [25], we improve the complexity of Index Calculus Algorithms in Elliptic Curves by means of Gröbner basis techniques and we analyze the complexity of this new approach by using the multi-homogeneous structure of the equations.

SECRET Project-Team

2.2. Highlights of the Year

- Extensive study of the hash function proposal Keccak, which has been chosen as the winner of the SHA-3 competition. The analysis of the algebraic properties of Keccak due to C. Boura and A. Canteaut is the best known result on the new hash function standard.
- Design of a variant of the McEliece public-key cipher based on a moderate density parity-check codes (MDPC). This family of codes leads to public keys with a reasonable size and does not weaken the underlying security proof.
- Construction of spatially coupled quantum LDPC codes which performs well under iterative decoding almost up to the coherent capacity of the quantum channel.

VEGAS Project-Team

2.2. Highlights of the Year

BEST PAPER AWARD :
[18] **Symposium on Computational Geometry - SoCG '12**. É. C. DE VERDIÈRE, G. GINOT, X. GOAOC.

ALF Project-Team

2.2. Highlights of the Year

- André Seznec has received the **first Intel Research Impact Medal** for "His exemplary work on high-performance computer micro-architectures, branch prediction, and cache architecture, have been of tremendous benefit to Intel, the industry, and the academic community as a whole.". (See http://www.intel.es/content/www/us/en/education/university/university-research-award.html).
- André Seznec has been elevated as an IEEE Fellow "for contributions to design of branch predictors and cache memory for processor architectures".

CAIRN Project-Team

2.2. Highlights of the Year

- Olivier Berder defended its "Habilitation à Diriger des Recherches (HDR)" thesis in 2012.

CAMUS Team

2.2. Highlights of the Year

- CAMUS takes part of the Laboratory of Excellence (LabEx) IRMIA (Institut de Recherche en Mathématiques, ses Interactions et Applications) whose proposal has been accepted by the french government.
- Alexandra Jimborean defended her PhD thesis September the 14th at the University of Strasbourg. She presented the first version of the dynamic and speculative code parallelizer VMAD (Virtual Machine for Advanced Dynamic analysis & transformation). Her jury was composed bu Albert Cohen (reviewer), Senior researcher at Inria, André Seznec (reviewer), Senior researcher at Inria, John Cavazos (reviewer), Professor at the University of Delaware, USA, François Bodin (examiner), Professor at the University of Rennes, Jean Christophe Beyler, HPC Software Engineer at Intel (examiner), Philippe Clauss and Vincent Loechner, advisors.
- Alain Ketterlin and Philippe Clauss published a paper on data dependence profiling at the The 45th Annual IEEE/ACM International Symposium on Microarchitecture [18].

2.5. Highlights of the Year

For 2012, from the point of view of organization, funding, collaborations, the main points to highlight are the following:

- Compsys II was positively evaluated in Spring 2012 by Inria. The evaluation committee members were Walid Najjar (University of California Riverside), Paolo Faraboschi (HP Labs), Scott Mahlke (University of Michigan), Pedro Diniz (University of Southern California), Peter Marwedel (TU Dortmund), and Pierre Paulin (STMicroelectronics, Canada), the last three assigned specifically to Compsys.
- Compsys prepared the installation in 2013 of Fabrice Rastello in the Giant center (Grenoble) with two PhD students and one post-doc, as a second component of Compsys. As already mentioned, this new organization is not fully validated yet.
- Compsys started a new industrial collaboration with Kalray, a multi-core french company, and the Inria team Parkas, through the ManyCoreLabs project coordinated by Kalray. The research activities are linked to compilation for the Kalray platform, in particular back-end code optimizations and compilation related to stream computing.
- Compsys obtained some important funding, mainly from the MI-LYON LaBex, to organize in Lyon a thematic quarter on compilation, languages, and architectures in 2013.

From a scientific point of view, the following points can be highlighted:

- Compsys finalized the developments in static single assignment (SSA) and register allocation, leading to the PhD defense of Quentin Colombet [1] and the habilitation of Fabrice Rastello [2].
- In high-level synthesis (HLS), the research and development efforts within the incubated start-up Zettice have been pursued and Zettice may become a full start-up in 2013.
- Compsys obtained several results in program analysis for parametric communication optimizations, scalable program termination, and dependence analysis for the X10 language.

For a detailed description of these new scientific results, see Section 6 “New Results”.

AOSTE Project-Team

2.2. Highlights of the Year

Aoste underwent its periodical Inria evaluation, as part of the Real-Time Embededded theme, in its eighth year of existence. Evaluation was very positive.

CONVECS Team

2.2. Highlights of the Year

- F. Lang and R. Mateescu's paper entitled "*Partial Model Checking Using Networks of Labeled Transition Systems and Boolean Equation Systems*" [15] was selected as one among the three "*best paper nominees*" of the TACAS 2012 conference, which had 36 papers published out of 147 submitted.
- At the end of 2012, the number of software licenses granted for the CADP toolbox since the beginning of its distribution has reached 10000.

DART Project-Team (section vide)

ESPRESSO Project-Team

2.4. Highlights of the Year

Polarsys is an Industry Working Group focusing on open source tools for the development of embedded systems. Polychrony was used to define the Tool Quality Assurance Plan of the Polarsys platform according to the DO-178B and DO-178C certification standards. Polychrony has been integrated in the experimental Polarsys platform.

Jean-Pierre Talpin received the ACM/IEEE LICS Test of Time Award for his paper “A type and effect discipline”, with his co-author Pierre Jouvelot.

MUTANT Project-Team

2.2. Highlights of the Year

The Antescofo software and programming language was featured in more than 15 world-premier creations and 30 events worldwide, including its premiers with *New York Philharmonics*, *Orchestre de Paris*, and prestigious venues in USA, Japan, Turkey, Poland, England and more. See website for more details.

PARKAS Project-Team (section vide)

POP ART Project-Team (section vide)

S4 Project-Team (section vide)

TRIO Project-Team

2.2. Highlights of the Year

- The release of the Open-PEOPLE platform.
- The organization of the 20th International Conference on Real-Time and Network Systems (RTNS2012).
- The acceptance of two TRIO papers to the two premier real-time conferences: the 33rd IEEE Real-time Systems Symposium (RTSS 2012) and the 24th Euromicro Conference on Real-Time Systems (ECRTS 2012).
- Successful completion of the TIMMO-2-USE project in September 2012 in which TRIO was leader of the work package on the algorithms and tools within the project.

VERTECS Project-Team

2.2. Highlights of the Year

The article [6] entitled Probabilistic omega-automata and co-authored by Nathalie Bertrand, together with Christel Baier and Marcus Grösser from TU Dresden, has been published in the Journal of the ACM. This article extends a paper published in 2008 in the proceedings of FoSSaCS, which received the EATCS best paper award, and already had a strong impact in the verification community.

ABSTRACTION Project-Team

2.2. Highlights of the Year

Antoine Miné was the program cochair and the local organizer of the 19th international statis analysis symposium (SAS 2012) in Deauville, September 11–13 2012 and Radhia Cousot is the program chair the 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2013) in Roma, January 23–25 2013.

ATEAMS Project-Team

2.2. Highlights of the Year

Paul Klint was awarded the CWI Fellowship, for lifetime contributions to science and CWI in particular. This distinction is given to prominent researchers at Centrum Wiskunde & Informatica (CWI) in Amsterdam for their contribution to CWI's research and administration.

Floor Sietsma defended her PhD on December 13, 2012. This makes her the *youngest PhD in Dutch academic history*, at 20 years old. Remarkably, Floor Sietsma has still two years of research time to go, for her thesis preparation took her about half of the allotted four years. NWO granted her a personalized grant on account of her unusual talents. Sietsma will stay at CWI and use the rest of her research grant to expand her research on the formal analysis of communication, exploring connections with data stream analysis, cryptography and agent technology in artificial intelligence.

CARTE Project-Team

2.2. Highlights of the Year

- We solved a problem that has been open for 15 years, relating three notions of complexity and information: Shannon information and entropy, Kolmogorov algorithmic information and Martin-Löf randomness [23].
- We developed a tool which is able to retrieve implementations of cryptographic primitives inside a trace of a binary. This result is published at CCS [22].
- We presented our work on behavioural malware detection using rewriting and model checking at ESORICS 2012 [20].
- For the Alan Turing year, we published an invited paper in the journal Phil. Trans. R. Soc. [16].

CASSIS Project-Team

2.4. Highlights of the Year

Cl-Atse Version 2.5-21 has been released by Mathieu Turuani. This efficient security protocol analyser offers advanced tracing options, supports set semantics as well as multiset one for modeling protocols, allows for Horn clause local deductions (for verifying assertions), and can handle in a complete and decidable manner negative constraints on the intruder's knowledge (for expressing non-disclosure policies).

CELTIQUE Project-Team (section vide)

COMETE Project-Team

2.2. Highlights of the Year

Mário Alvim, an ex PhD student of Comète who defended his thesis in October 2011, has been nominated for the “Prix de thèse ParisTech 2012”.

CONTRAINTES Project-Team (section vide)

DEDUCTEAM Team (section vide)

FORMES Team

2.2. Highlights of the Year

- The automated termination prover HOT developed by Frédéric Blanqui won the 2012 termination competition in the category “higher-order rewriting union beta”.

GALLIUM Project-Team

2.2. Highlights of the Year

Xavier Leroy was awarded the 2012 Microsoft Research Verified Software Milestone Award in recognition of his work on the CompCert C verified compiler.

MARELLE Project-Team

2.2. Highlights of the Year

This year, the Mathematical Components project of the Microsoft Research-Inria joint center under the direction of Georges Gonthier completed the major objective it had set six years ago: the complete formal verification of the Odd Order theorem, also known as the Feit Thompson theorem, which states that every odd order finite group is solvable. The Marelle project-team is a key participant in this project.

For more information : http://www.msr-inria.inria.fr/Projects/math-components/feit-thompson

MEXICO Project-Team (section vide)

PAREO Project-Team

2.2. Highlights of the Year

BEST PAPER AWARD :
[14] **Turing-100, The Alan Turing Centenary Conference**. S. STRATULAT.

PARSIFAL Project-Team

2.2. Highlights of the Year

- Stefan Hetzl received his Habilitation 5 November 2012 from the Technical University of Vienna.
- Kaustuv Chaudhuri and Stefan Hetzl organized "Collegium Logicum 2012: Structural Proof Theory" at Inria-Saclay.
- Dale Miller and Gopalan Nadathur (Professor at the University of Minnesota) published a book title "Programming with higher-order logic" (June 2012, Cambridge University Press).

PI.R2 Project-Team (section vide)

PROSECCO Project-Team

2.2. Highlights of the Year

This year, we published 5 articles in international journals and 11 articles in peer-reviewed international conferences, including presitigious conferences such as CCS (1), CRYPTO (1), and CSF (2). In addition to these, we published 1 HDR thesis, 3 master's theses, 4 technical reports, and 5 workshop papers. We also have 4 articles already accepted for publication in international conferences in 2013.

We released updates to 3 verification tools and released 3 new software packages. We discovered and reported major security vulnerabilites in dozens of commercial software packages, hardware devices, and websites.

Of our work published in 2012, we would like to highlight the following:

- Our paper in CRYPTO 2012 [22] describing new attacks on cryptographic hardware devices, which got significant interest from both the cryptographer community and from the press.
- Our work on generating implementation code from verified models of cryptographic protocols [26], [27].
- Our work on formally analyzing web application security using automated verification tools, which uncovered major attacks in popular websites and web browsers [21], [24], [20].

SECSI Project-Team

2.2. Highlights of the Year

- Workshop celebrating the 15th anniversary of LSV (the lab where SECSI is hosted) and Jean Goubault-Larrecq's CNRS silver medal, ENS Cachan, February 06-07, 2012 (http://www.lsv.ens-cachan.fr/Events/LSV15Y/)
- The ANR project AVOTÉ on the formal analysis of electronic voting protocols (http://www.lsv.ens-cachan.fr/Projects/anr-avote/) has been nominated to receive a price awarded by the ANR.

TASC Project-Team

2.2. Highlights of the Year

1. The IBEX library has been entirely re-factored from scratch to provide a more clean and easy-to-use interface as well as a more powerful engine and made available in December 2012 on multiple platforms (Linux, MacOs, Windows). Global optimization and system solving front-end algorithms have been tested on more than 500 benchmarks.
2. Significant advance on learning constraints models for highly structured problems was done in 2012. The system [19] is based on the global constraint catalog, providing the library of constraints that can be used in modeling, and the Constraint Seeker tool, which finds a ranked list of matching constraints given one or more sample call patterns. Surprisingly, the system often finds usable models even when working with a single, positive example.

TOCCATA Team

2.2. Highlights of the Year

A major event in the life of our team this year is naturally its creation, as a refoundation of the former ProVal team, starting officially on September 1st, with C. Marché as a new leader. This report indeed covers all the activities of the team in 2012, including the activities of ProVal from January to August.

Another important event is the arrival of Arthur Charguéraud as a new “Chargé de Recherche”, since October.

The current section and the next one present the scientific foundations, objectives and axes of research of the new team. The theme of verification of numerical programs, that took importance in the former project, is now a major axis. We also emphasize a new axis of research concerning the certification of tools.

TYPICAL Project-Team

2.2. Highlights of the Year

Assia Mahboubi, Enrico Tassi and Cyril Cohen were among the main participants in the project of formalization of the Feit-Thompson (Odd Order) theorem finally completed in September 2012 by the Mathematical Components team (lead by Georges Gonthier).

Bruno Barras and Assia Mahboubi have been granted fellowships by the Insititute for Advanced Study (Princeton, USA).

VERIDIS Project-Team (section vide)