Activity Report 2011

Section highlights of the Team
# Algorithms, Certification, and Cryptography

1. **ALGORITHMS Project-Team** ......................................................... 5
2. **ARENAIRE Project-Team** .................................................... 6
3. **CARAMEL Project-Team** ....................................................... 7
4. **CASCADE Project-Team (section vide)** ...................................... 8
5. **GALAAD Project-Team (section vide)** ..................................... 9
6. **GEOMETRICA Project-Team** .................................................. 10
7. **LFANT Project-Team** .......................................................... 11
8. **SALSA Project-Team** .......................................................... 12
9. **SECRET Project-Team** ......................................................... 13
10. **TANC Project-Team** ........................................................... 14
11. **VEGAS Project-Team (section vide)** .................................... 15

## Architecture and Compiling

12. **ALF Project-Team** ............................................................ 16
13. **CAIRN Project-Team** ......................................................... 17
14. **CAMUS Team** ................................................................. 18
15. **COMPSYS Project-Team** ................................................... 19

## Embedded and Real Time Systems

16. **AOSTE Project-Team** ......................................................... 20
17. **DART Project-Team** .......................................................... 21
18. **ESPRESSO Project-Team** .................................................. 22
19. **LICT Exploratory Action** .................................................... 23
20. **PARKAS Team** ................................................................. 24
21. **POP ART Project-Team (section vide)** .................................. 25
22. **S4 Project-Team** .............................................................. 26
23. **TRIO Project-Team** ........................................................... 27
24. **VASY Project-Team** ......................................................... 28
25. **VERTECS Project-Team** .................................................... 29

## Programs, Verification and Proofs

26. **ABSTRACTION Project-Team** ............................................. 30
27. **ATEAMS Project-Team** ..................................................... 31
28. **CARTE Project-Team (section vide)** .................................... 32
29. **CASSIS Project-Team** ....................................................... 33
30. **CELTIQUE Project-Team** .................................................. 34
31. **COMETE Project-Team** ..................................................... 35
32. **CONTRAINTES Project-Team (section vide)** .......................... 36
33. **FORMES Team (section vide)** ............................................ 37
34. **GALLIUM Project-Team** .................................................... 38
35. **MARELLE Project-Team** .................................................... 39
36. **MEXICO Project-Team** ...................................................... 40
37. **MOSCOVA Project-Team** .................................................. 41
38. PAREO Project-Team (section vide) .............................................................. 42
39. PARSIFAL Project-Team ................................................................. 43
40. PLR2 Project-Team (section vide) ......................................................... 44
41. PROVAL Project-Team ................................................................. 45
42. SECSI Project-Team ................................................................. 46
43. TASC Project-Team ................................................................. 47
44. TYPICAL Project-Team (section vide) .................................................. 48
45. VERIDIS Team ................................................................. 49
2.2. Highlights

Philippe Flajolet, head of the project and of former related projects at Inria, died suddenly on March 22. He is celebrated for opening new lines of research in analysis of algorithms, developing powerful new methods, and solving difficult open problems. A conference with more than 250 participants has been organized by the project in December. It will pay homage to the man as well as the multi-faceted mathematician and computer-scientist.
2.2. Highlights

BEST PAPER AWARD:

CARAMEL Project-Team

2.2. Highlights

The highlights for year 2011 in the CARAMEL team are

- the successful organization of the ECC conference, that gathered more than 120 participants;
- the publication of the major result of Robert and Lubicz on explicit isogenies in the prestigious journal Compositio Mathematica.
CASCADE Project-Team (section vide)
GALAAD Project-Team (section vide)
2.2. Highlights

We organized the 27th Annual Symposium on Computational Geometry (SoCG 2011) in Paris: http://socg2011.inria.fr/. This is the main conference in the field. We also organised a summer school entitled “Computational Geometric Learning” at the IHP in Paris, to foster connections between Computational Geometry and Machine Learning. About 70 persons attended.

Mariette Yvinec and Pierre Alliez, together with Jane Tournois and Laurent Rineau from the INRIA spin-off Geometry Factory, received the Meshing Maestro Award at the 20th International Meshing Roundtable for their poster “Meshing with CGAL”.

Bertrand Pellenard and Pierre Alliez, together with Jean-Marie Morvan from University Lyon1/CNRS and King Abdullah University of Science and Technology, received the Best Technical Poster Award at the 20th International Meshing Roundtable for their poster “Isotropic 2D Quadrangle Meshing with Size and Orientation Control”.

2.2. Highlights

- With PARI/GP 2.5.0, the first major stable release of the software since 2007 has been made in June 2011.
- In March 2011, the MPC software has become an official GNU package with Andreas Enge as its maintainer.
SALSA Project-Team

2.2. Highlights

- **Computer Algebra.** Best Poster Award STOC 2011 (San Jose, USA) – PWE : Polynomial with Errors.
- **ANR Grants** Two new projects (HPAC and GEOLMI) were accepted (4 years projects).
- **Maple.** Maple 15 release : the contract with Maple was renewed until Dec. 2011.
SECRET Project-Team

2.2. Highlights

- **Cryptanalysis of several hash functions proposed to the SHA-3 competition**: this international competition, launched by the American National Institute of Standards and Technology, aims at selecting a new standard for hash functions\(^1\). The revision of the current standard FIPS 180-2 has actually been decided by NIST in response to the recent attacks against almost all existing hash functions (e.g. MD5, SHA-0, SHA-1). Among the 64 hash function proposals submitted to the SHA-3 competition, several candidates have been cryptanalyzed by some researchers of the project-team. More recently, we have provided a deep study of the algebraic properties of some of the finalists of the competition.

- **Discovery of a distinguishing property for the family of Goppa codes** which are used in the original McEliece cipher and the CFS signature scheme. Even if it does not lead to an attack, this property invalidates the previously known security proofs of these systems. Among the many families of linear codes which have been considered for code-based cryptography, Goppa codes seemed to be the only safe one. Now even Goppa codes seem to be questioned.

- **Organization of the WCC international conference**, which was held in Paris in April 2011. This was the seventh in the series of biannual workshops on *Coding and Cryptography*.

\(^1\)http://csrc.nist.gov/groups/ST/hash/sha-3/
2.3. Highlights

**Best Paper Award:**

VEGAS Project-Team (section vide)
ALF Project-Team

2.2. Highlights

André Seznec has been awarded an ERC advanced investigator grant for 2011-2016 called DAL, Defying Amdahl’s Law.

André Seznec won the 3rd Championship Branch Prediction in both the conditional branch prediction track and the indirect branch prediction track.
2.2. Highlights

Daniel Menard and Steven Derrien defended their "Habilitation à Diriger des Recherches (HDR)" thesis in 2011.
CAMUS Team

2.2. Highlights

- The Associate Team Ancome, regrouping Camus and their Argentinian partners from the LaFhis team of the University of Buenos Aires, has started officially its activities in January 2011.


- Benoît Pradelle defended his PhD thesis December the 20th 2011 at the University of Strasbourg. He presented his results on dynamic selection of parallel code versions, automatic parallelization of binary codes and polyhedral dynamic and speculative parallelization. His jury was composed by Albert Cohen (reviewer), from INRIA, Sanjay Rajopadhye (reviewer), Colorado State University, USA, John Cavazos (examiner), University of Delaware, USA, Philippe Clauss, Alain Ketterlin and Vincent Loechner (advisors).

- Alexandra Jimborean received the best poster award at the international conference Code Generation and Optimization (CGO) that was held in Chamonix, France, in April 2011.
2.4. Highlights

The year 2011 was marked by strong financial difficulties due to the unilateral decision of the government to stop all Nano2012 fundings. For Compsys, involved in the Mediacom and S2S4HLS projects, this has led to a non-anticipated budget cut of about 60% (excluding salaries). The help of Inria to support the salary of Florian Brandner (post-doc/engineer) and pay some registration fees (in particular CGO’11) was crucial. The research activities in Mediacom still continue, but in a restricted form, until the end of Quentin Colombet’s PhD. However, Compsys had to stop its participation to S2S4HLS.

Compsys continued its activities on static single assignment (SSA) and register allocation, as well as on high-level synthesis (HLS) for FPGA. The main achievements in 2011 are:

- The design of a tree-scan allocator was continued and two related contributions were published at SCOPES’11 and CASES’11.
- Our new algorithm for liveness analysis under SSA and a comparison with existing methods were finalized and published at APLAS’11.
- An analysis, based on an integer linear programming formulation, of “optimal spilling” was made with full experiments and published at CASES’11.
- The automatic generation of double-buffered pipelined versions of computation kernels for FPGA was improved and will be presented at PPoPP’12. A simplifier for Boolean affine formulas was designed that should improve the code generation part.
- Alexandru Plesco, following his PhD, initiated a project of start-up, Zettice, supported by Inria and ENS-Lyon, combining the experience of Compsys on compilation and HLS, and the expertise of Arénaire on floating-point pipelined operators for FPGA. A publication at ARC’11 illustrates this effort.

Also, in 2011, Compsys was very active in the organization of important events for our scientific community:

- Fabrice Rastello, after re-activating the french community in compilation, was very involved in the organization of the main international conference in code generation (CGO’11), in Chamonix, and the organization and advertising of its workshops.
- Christophe Alias was the main organizer of IMPACT’11 (international workshop on polyhedral compilation techniques), held in conjunction with CGO’11. This workshop is the very first international event on this topic. Laure Gonnord was co-organizer of the workshop ACCA’11 (analyze to compile, compile to analyze), also part of CGO’11.

Best Paper Award:
2.2. Highlights

Robert de Simone was made Honorary Professor of the Software Engineering Institute (SEI) at East China Normal University (ECNU) in Shanghai.
2.2. Highlights

The International Conference on Computer Design encompasses a wide range of topics in the research, design, and implementation of computer systems and their components. ICCD’s multi-disciplinary emphasis provides an ideal environment for developers and researchers to discuss practical and theoretical work covering system and computer architecture, verification and test, design and technology, and tools and methodologies. This conference exists from 30 Years. The paper (“Hybrid System Level Power Consumption Estimation for FPGA-Based MPSoC”) of the PhD student Santosh Rethinagiri obtained the best paper award 2011.

Best Papers Awards:

ESPRESSO Project-Team

2.4. Highlights

The main headline of 2011 is the release of the Polychrony toolset in open-source under GPL v2.0 and EPL licenses in July. It is the result of a process initiated several years ago and conducted in close collaboration with INRIA’s DTI in order to precisely define the perimeter of the license and identify the best-suited licensing terms compatible with its users and potential contributors.
2.2. Highlights

The main results of the year concern both the aforementioned research and networking objectives:

- Integration of technical and legal requirements in a common framework to reduce legal uncertainties in software liability [5].
- Definition of a formal language for the specification of obligations and a posteriori verification of legal rules [10].
- Co-organization of a multidisciplinary conference on digital evidence (Palais de Justice de Paris, 8 December 2011) ¹.
- Organization of a multidisciplinary workshop on legal and technical aspects of causality (EN SCP Paris, 7 December 2011) ².
- Co-organization of the CPDP Conference and panel on “behavioural targeting” ³. CPDP, which is now established as the main privacy conference in Europe, attracts every year a wider and more multidisciplinary audience (more than 300 participants in 2011).

¹ http://licit.inrialpes.fr/lise/
² http://licit.inrialpes.fr/lise/
³ http://www.cpdpconferences.org
PARKAS Team

2.1. Highlights

- Tobias Grosser has been awarded a Google European Doctoral Fellowship, a highly competitive 3 years scholarship of 120k € (14 recipients in 2011).
POP ART Project-Team (section vide)
2.2. Highlights

The three main achievements of the S4 team during 2011 are:

- The non-standard semantics of hybrid systems (Section 6.2) and its application to the compilation of hybrid data-flow synchronous languages.
- The modal interface theory (Section 6.3) and its implementation in the Mica toolbox (Section 5.1).
- Several results on the separability and the distributability of Petri nets (Section 6.1).
TRIO Project-Team

2.2. Highlights

+ "PROARTIS: Probabilistically Analyzable Real-Time Systems" was accepted for publication in "ACM Transactions in Embedded Computing Systems". This paper, co-authored by Liliana Cucu-Grosjean, Luca Santinelli and Codé Lo from the team, is a position paper that results from the work undertaken within the Proartis European project.

+ Nicolas Navet is co-head of the High Performance Embedded Systems (HPES) cluster of GDR CNRS ASR and co-animator of Actriss group (real-time services and infrastructure) of HPES cluster.

+ Startup Alphability has been created to provide risk management solutions and is laureate of the 13th national contest for the creation of innovative technology companies organized by the Ministry of Higher Education and Research ("Création/Développement" category).

+ Three patents in the field of automotive communication systems have been filled in together with PSA Peugeot-Citroën.

+ The Open-PEOPLE software platform, a federative platform aiming at providing energy measurement, modelling and optimization capabilities for software systems, saw the first release of its module giving access and control to the distant hardware platform for actual experimentations.
VASY Project-Team

2.2. Highlights

In 2011, Hubert Garavel received the prestigious Humboldt Research Award granted by the Alexander von Humboldt foundation (Bonn, Germany).
VERTECS Project-Team

2.2. Highlights

FoSSaCS paper [18] and TACAS paper [17] seriously improve the state of the art and may have a strong impact. [18] proposes an approximate determinization procedure for timed automata, successfully adapted in [17] for off-line test generation from timed automata, and is promising for other observability problems (diagnosis, implementability,...).
2.2. Highlights

The paper “Static Analysis and Verification of Aerospace Software by Abstract Interpretation”, written by the team [1], has been selected in 2011 by the AIAA Intelligent Systems Technical Committee as the Best Paper from the AIAA 2010 Infotech@Aerospace Conference.

The MemCAD ERC Starting Grant (“Memory Compositional Abstract Domains”) was started on October, 1st, 2011 (funded by the European Research Council “IDEAS” programme).
2.2. Highlights

- **Professorship** Jan van Eijck was appointed Professor at Universiteit van Amsterdam.
- **Distinguished scientist** In August Michael Godfrey joined us for a year of his sabbatical from University of Waterloo (Canada).
- **Rascal release** A new version of the Rascal meta-programming language was released in October.
- **Forensics** The Derric domain specific language generates faster and more accurate implementations than its competitors in the digital forensics arena, using less than 1500 lines of code.
- **Inception of Ensō** In a collaboration with University of Texas, Tijs van der Storm introduced the Ensō framework: a new form of programming based on the concepts of model driven engineering.
- **Eclipse** The source code of Rascal was approved for inclusion in the Eclipse IMP source code and releases.
CARTE Project-Team (section vide)
CASSIS Project-Team

2.4. Highlights

Véronique Cortier has received a *starting grant* from the European Research Council (ERC). Her project, called *ProSecure* (Provably secure systems: foundations, design, and modularity), has started in 2011 for five years. Steve Kremer, formerly in the Secsi project-team, has joined Cassis since September 1. Véronique Cortier and Steve Kremer have edited a book on formal models for analysing security protocols [64]. Laurent Vigneron has defended his habilitation on the application of automated deduction to the verification of infinite systems [17].
2.2. Highlights

Sandrine Blazy received the 2011 La Recherche award in Information Sciences for her contributions to the CompCert verified C compiler, together with Zaynah Dargaye, Xavier Leroy and Jean-Baptiste Tristan.
COMETE Project-Team

2.2. Highlights

+ Catuscia Palamidessi has been keynote speaker at the 2011 edition of the conference ICALP (International Colloquium on Automata, Languages and Programming, http://icalp11.inf.ethz.ch/).
CONTRAINTES Project-Team (section vide)
FORMES Team (section vide)
GALLIUM Project-Team

2.2. Highlights

Xavier Leroy (EPI Gallium), Sandrine Blazy (EPI Celtique), Zaynah Dargaye (CEA) and Jean-Baptiste Tristan (Oracle Labs) were awarded the 2011 *La Recherche* prize in Information Sciences for their work on the CompCert verified compiler.
2.1. Highlights

Our work on formal proofs for cryptography now receives attention in best conferences of specialists of that domain.

**BEST PAPER AWARD:**

2.2. Highlights

The article "Synthesis and Analysis of Product-form Petri Nets" by Serge Haddad, Jean Mairesse and Hoang-Thach Nguyen received the Best Paper Award at the International Conference on Theory and Application of Petri Nets (ICATPN) 2011 in Newcastle, UK.

For a large Markovian model, a "product form" is an explicit description of the steady-state behaviour which is otherwise generally untractable. Being first introduced in queueing networks, it has been adapted to Markovian Petri nets. Here we address three relevant issues for product-form Petri nets which were left fully or partially open: (1) we provide a sound and complete set of rules for the synthesis; (2) we characterise the exact complexity of classical problems like reachability; (3) we introduce a new subclass for which the normalising constant (a crucial value for product-form expression) can be efficiently computed.
2.2. Highlights

Moscova is proud of producing the following important results in 2011:

- 1 PhD was defended, another one will be defended on February 8, 2012.
- 1 paper accepted at POPL 2012 (1 paper was accepted at POPL 2011).
PAREO Project-Team (section vide)
2.2. Highlights

- Josh Hodas and Dale Miller won the 2011 LICS Test of Time Award for their 1991 paper titled “Logic programming in a fragment of intuitionistic linear logic.”
- Dale Miller’s proposal titled “ProofCert: Broad Spectrum Proof Certificates” submitted to the ERC Advanced Investigator Grant in 2011 was accepted and will be funded for 2012-1016.
PL.R2 Project-Team (section vide)
2.2. Highlights

A new trend emerging in 2010-2011 is the construction of international program verification benchmarks and program verification competitions. Benchmarks include the VACID0 challenges (http://vacid.codeplex.com/) and the VerifyThis collection (http://verifythis.cost-ic0701.org/). We took our part in these efforts by proposing our own gallery of verified programs (http://proval.lri.fr/gallery/index.en.html). Regarding competitions, we proposed our own solutions to the first (informal) VSTTE competition (http://proval.lri.fr/gallery/vscomp2010.en.html), we participated to the first FoVeOOS competition (Turin, Italy, Sep. 2011) and were ranked as first, ex-aequo with two other teams (http://proval.lri.fr/gallery/cost11comp.en.html) and last but not least, we indeed organized the first formal VSTTE program verification competition (November 2011, https://sites.google.com/site/vstte2012/compet).


**BEST PAPER AWARD:**

2.2. Highlights

- Jean Goubault-Larrecq was awarded the CNRS Silver Medal, 2011.
- SECSI organized the 24th IEEE Computer Security Foundations Symposium (CSF).
- SECSI organized a two-day colloquium centered around several invited talks and three defenses of habilitation theses by members of SECSI.
- Steve Kremer co-edited, with Véronique Cortier, the book *Formal Models and Techniques for Analyzing Security Protocols* [47].
2.2. Highlights

- **Best student paper** for M. Pelleau et al. at the 17th International Conference on Principles and Practice of Constraint Programming (CP 2011) for *Octogonal Domains for Continuous Constraints* (see [22]).

- **Google Focused Research Awards** (see item Mathematical Optimization) for providing explanation-based user-oriented features in constraint solvers given to N. Jussien.


**Best Paper Award:**
TYPICAL Project-Team (section vide)
VERIDIS Team

2.2. Highlights

- Marie Duflot-Kremer joined VeriDis in September 2011. Previously at University Paris Est Créteil, she is an assistant professor at University Henri Poincaré Nancy 1. Her research is centered around statistical model checking and the verification of probabilistic systems.

- The veriT solver (see section 5.1) entered for the third time the international competition of SMT solvers, SMT-COMP 2011, a joint event with the SMT workshop 2011 and the CAV conference. It implemented a new original technique (presented at CADE 2011) that greatly improves efficiency on some categories of benchmarks. Several competitors also implemented this technique, as for instance the winner of the competition on those categories (Z3).

- Pascal Fontaine (VeriDis) and Aaron Stump (University of Iowa) organized the first workshop on Proof eXchange for Theorem Proving, co-located with CADE 2011. The workshop was well attended and we believe that this series of events will stimulate research in the area, and will lead to important improvement in reasoning techniques.