RESEARCH CENTER
Paris - Rocquencourt

FIELD

Activity Report 2013

Section highlights of the Team

Edition: 2014-03-19

AXIS Project-Team

2.2. Highlights of the Year

- Y. Lechevallier gave an **invited talk** "Partitioning Methods On Dissimilarity Matrices Set" related to this publication [20] (cf. Section 6.2.8) at the First European Conference on Data Analysis (ECDA 2013) (with around 300 participants) jointly hosted by the two Classification Societies (GkKI in Germany and SFC in France) in July at Luxembourg.
- **BIOVISION 2013**, the World Life Sciences Forum: B. Trousse was invited as **panellist** in the prospective session "eHealth: a coming medical revolution?" at the major event BIOVISION 2013, held March 24-26, 2013 in Lyon, France. With over 3,000 participants, 200 high-level speakers and more than 30,000 Internet followers, BIOVISION is the most-attended multi-stakeholder meeting for all life sciences'players. B. Trousse illustrated the notion of living lab with three concrete e-health experiences from three French living labs (Autonom'lab - Limousin, e-care - Lyon, Living Lab High Alps Living Lab -05) and argued on the importance for the public authorities to appropriate this type of instruments which are living labs;
- **2030 Prospective (ADEME)**: B. Trousse was invited by ADEME and Chronos firm among relevant interdisciplinary experts for analysing the ICT & Building challenges at 2030 horizon and for participating at one 2-days seminar at ADEME (Sophia Antipolis);
- **MyGreenServices - Good Practice Prize** (Category: Project proposals, initiatives, methodologies and studies) by the **International Design for All Foundation** for Awards 2014 which will be at Paris in February 2014; AxIS managed a complete deployment of a Living Lab Experiential Design process involving more than 50 active citizen and 13 citizen pollution fixed and mobile sensors. The impact in terms of behaviour change using MyGreenServices was very promising;
- **FocusLab Platform (CPER Telius 2010-2013)**: we completed a first web-based application allowing the reservation of hardware, software or books (cf. Section 6.6);
- **Signature of a Memorandum of Understanding** (MoU) between B. Trousse, President of France Living Labs as Inria representative of ICT Usage Lab and Jarmo Eskelinen, Chair of ENoLL the European Network of Living Labs;
- D. Robache is member of the Department of Research Team Assistants of Inria Sophia Antipolis which receives the Research Support Department Inria Award in 2013.

ABSTRACTION Project-Team

2.2. Highlights of the Year

Patrick and Radhia Cousot have received in 2013 the SIGPLAN Achievement award, for the invention, development, and application of abstract interpretation http://www.sigplan.org/Awards/Achievement/Main.

AOSTE Project-Team

2.2. Highlights of the Year

The 2013 edition of the RTNs conference was organized in Sophia-Antipolis, with Robert de Simone as General Chair and Liliana Cucu-Grosjean as keynote speaker. Rob Davis, from the University of York, was granted a five-year Inria International Chair position in our team at Rocquencourt.

CASCADE Project-Team (section vide)

CONTRAINTES Project-Team (section vide)

CRYPT Team

2.3. Highlights of the Year

Phong Nguyen and Xiaoyun Wang obtained a 973 grant from China's Ministry of Science and Technology (MOST): the so-called 973 grants are China's largest grants for fundamental research.
BEST PAPER AWARD :
[19] **ISSAC '13 - 38th international symposium on International symposium on symbolic and algebraic computation**. J. BI, Q. CHENG, M. ROJAS.

DEDUCTEAM Exploratory Action

2.3. Highlights of the Year

The Version 2 of Dedukti has been released. Gilles Dowek has been invited speaker to CSR, Hapoc, and to the Colloquium of the University Pierre et Marie Curie. David Delahaye has been an invited speaker of PSATTT.

FORMES Team

2.3. Highlights of the Year

The project has released a new version of its **SimSoC** simulation software, as an open source software release 0.8, available from http://gforge.inria.fr/projects/simsoc/

GALLIUM Project-Team

2.2. Highlights of the Year

Didier Le Botlan (INSA Toulouse) and Didier Rémy received the ACM SIGPLAN Most Influential ICFP Paper Award for their ICFP 2003 paper, *MLF: Raising ML to the power of System F* [44].

MUTANT Project-Team

2.2. Highlights of the Year

Figure 2. Antescofo presentation and demo in Bercy, Ministry of Industry.

Antescofo has been awarded the Industry prize by the French Minister of Industry, for its R&D and upcoming industrial applications.

Antescofo has been presented at the MIF Show (salon Made In France) invited by the ministère du redressement productif (November 2013).

Invited Demonstration at the 10th anniversary of La Recherche Prize.

PARKAS Project-Team

2.2. Highlights of the Year

Robin Morisset was Awarded a Google Doctoral Fellowship.

Louis Mandel and Marc Pouzet received a reward for the paper introducing the ReactiveML language for the first time and presented at the French conference JFLA 2005 (“On the occasion of this quarter century, the program committees and steering selected four outstanding contributions from the articles published in JFLA past decade.")

Louis Mandel has been hired in Sept. 2014 at Collège de France, as an Assistant Professor.

PI.R2 Project-Team

2.2. Highlights of the Year

The Coq team received the 2013 ACM SIGPLAN Programming Language Software Award, which was presented at POPL'14 in San Diego. To quote: "The Programming Languages Software Award is given by ACM SIGPLAN to an individual or an institution to recognize the development a software system that has had a signicant impact on programming language research, implementations, and tools. The impact may be reflected in the wide-spread adoption of the system or its underlying concepts by the wider programming language community either in research projects, in the open-source community, or commercially."

POLSYS Project-Team

2.2. Highlights of the Year

- Mohab Safey El Din was invited speaker in the International Symposium on Symbolic and Algebraic Computation (ISSAC), held in Boston, June 26-29, 2013.
- In [6] we investigate the security of HFE and Multi-HFE schemes. Our attacks are based on solving the MinRank problem. We prove that they are polynomial in the degree of the extension field for all possible practical settings used in HFE and Multi-HFE.
- In [11] we consider an algorithm to solve the DLP problem on Edwards curves, which are a well-known family of elliptic curves. We exploit the symmetries and the structure of twisted Edwards and twisted Jacobi intersections curves to gain an exponential factor $2^{\omega(n-1)}$ in the complexity bound where ω is the exponent of matrix multiplication.
- In [17] we give an explicit upper bound for the algebraic degree and an explicit lower bound for the absolute value of the minimum of a polynomial function on a compact connected component of a basic closed semialgebraic set when this minimum is not zero and is attained.

PROSECCO Project-Team

2.2. Highlights of the Year

This year, we published 6 articles in international journals and 11 articles in peer-reviewed international conferences, including presitigious conferences such as IEEE S&P (1), ACM CCS (2), Usenix Security (1), ESORICS (2), and POST (3). In addition to these, we published 1 PhD thesis and several technical reports. We also have 3 articles already accepted for publication in international conferences in 2013: POPL (2), NDSS (1).

We released updates to several verification tools and software packages. We discovered and reported major security vulnerabilites in dozens of commercial software packages, hardware devices, and websites. The work of our group also spun-off a new startup company created by Graham Steel, and we continue to collaborate with this startup.

Of our work published in 2013, we would like to highlight the following:

- Our paper in IEEE S&P 2013 [21] presents the first cryptographically verified implementation of TLS.
- Our work on the computational analysis of cryptographic protocols yielded new results and major publications [19], [26].
- Our work on formally analyzing web application security uncovered major attacks on browsers and websites and proposed novel language-based verified solutions [20], [29], [25].

SECRET Project-Team

2.2. Highlights of the Year

- *Cryptanalysis of several recently proposed lightweight block ciphers:* The area of lightweight primitives has drawn considerable attention over the last years, due to the need for low-cost cryptosystems for several emerging applications like RFID tags and sensor networks. The strong demand from industry has led to the design of a large number of lightweight block ciphers, with different implementation features. In this context, the need for a significant cryptanalysis effort is obvious. The demand from industry for clearly recommended lightweight ciphers requires that the large number of these potential candidates be narrowed down. In this context, the project-team has obtained cryptanalytic results on several recently proposed lightweight block ciphers, including an attack against the full cipher KLEIN-64, the best known attack against a round-reduced version of PRINCE, and some distinguishers on the internal permutation of LED.
- *Cryptanalysis of a variant of the McEliece public-key cryptosystem based on some wild Goppa codes:* The original McEliece cryptosystem proposed in 1978 uses the class of classical binary Goppa codes as private codes. Many other classes of codes have been suggested since the original proposal, but most of them have been cryptanalysed, while the class of Goppa codes still resists all structural attacks. Then, the use of a more general family of Goppa codes over $\mathbf{F}_q$, $q \geq 2$, named wild Goppa codes, has been proposed in 2010 by Bernstein *et al.* in order to reduce the key size of the system. Our recent work leads to an attack which allows to recover the private key in polynomial time when wild Goppa codes over a quadratic finite field extension are used. This is the very first structural attack of the McEliece cryptosystem when some Goppa codes are used. The key-point in the attack is the behaviour of these codes with respect to component-wise product of codes. A similar technique has also been exploited for breaking some other variants of the McEliece system, including one based on Reed-Solomon codes.
- *Experimental demonstration of long-distance continuous-variable quantum key distribution:* Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications. The rapid progress in this field has enabled quantum key distribution in real-world conditions and commercial devices are now readily available. Quantum key distribution systems based on continuous variables provide the major advantage that they only require standard telecommunication technology. However, to date, these systems have been considered unsuitable for long-distance communication. In collaboration with experimental groups, we have overcome all previous limitations and demonstrated for the first time continuous-variable quantum key distribution over 80 km of optical fibre. Our results correspond to an implementation guaranteeing the strongest level of security for quantum key distribution reported so far for such long distances and pave the way to practical applications of secure quantum communications.

CAD Team (section vide)

CLASSIC Project-Team (section vide)

GAMMA3 Project-Team (section vide)

MATHRISK Project-Team

2.2. Highlights of the Year

- AA. Sulem has been invited for a Plenary talk at IFIP TC 7 Conference on System Modelling and Optimization, Klagenfurt, Austria. September 2013 - http://ifip2013.uni-klu.ac.at/

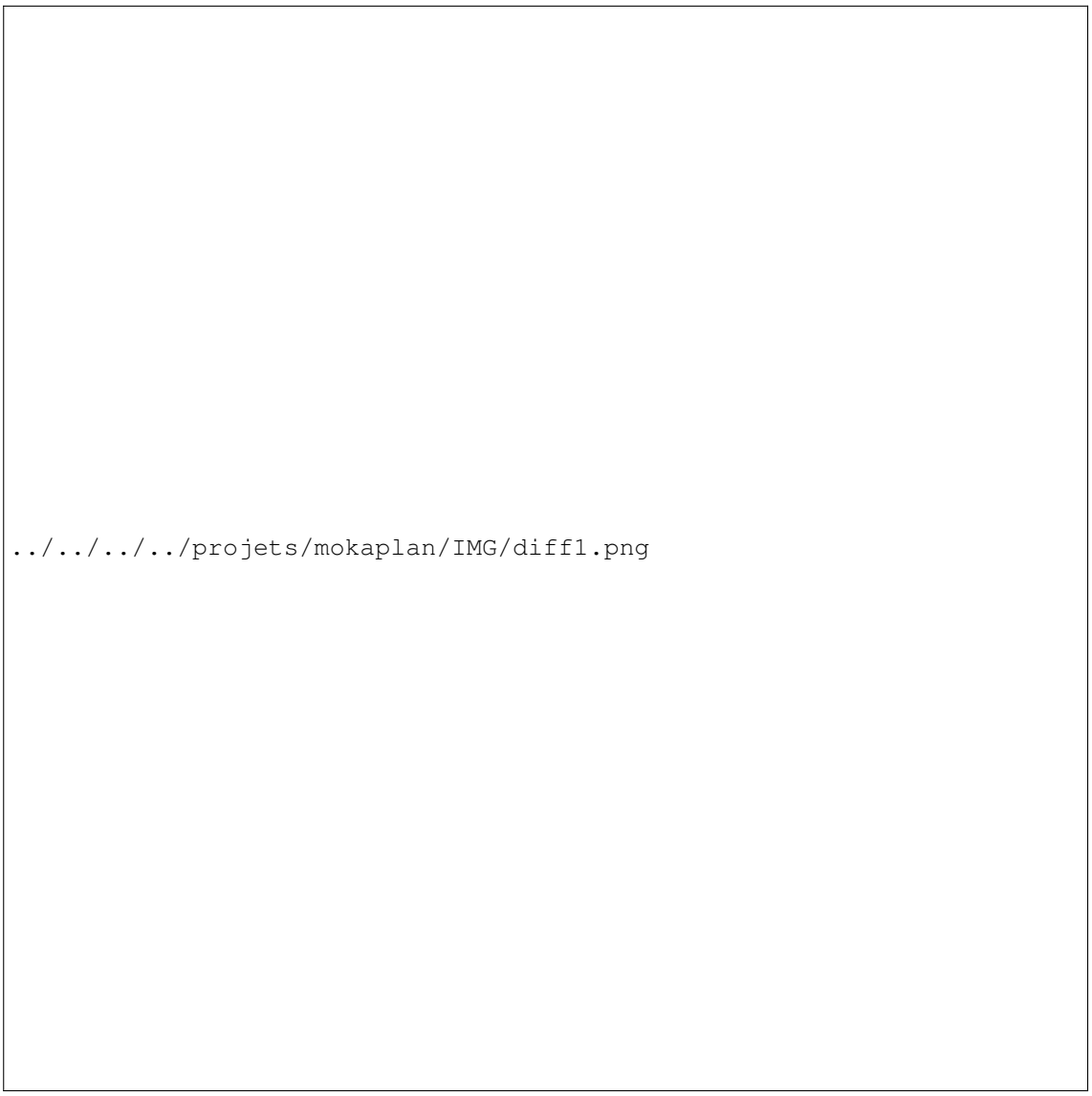
- The paper of B. Jourdain with S. Méléard and W. Woyczynski "Lévy flights in evolutionary ecology", *Journal of Mathematical Biology*, has been honored by the prize La Recherche - Mathématiques 2013 - http://www.leprixlarecherche.com/palmares-2013

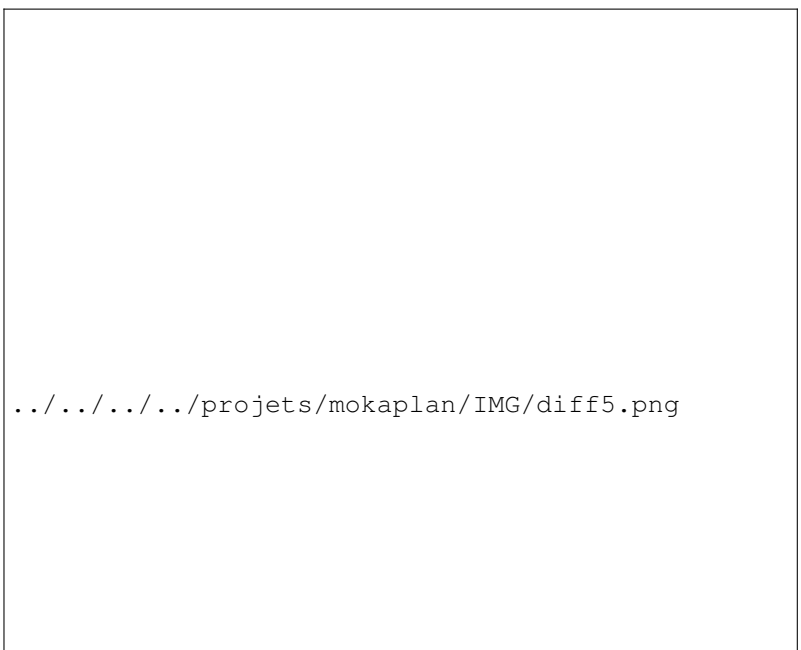
MICMAC Project-Team (section vide)

MOKAPLAN Exploratory Action

2.2. Highlights of the Year

The paper [6] resolves numerically the Monge-Ampère formulation of the Optimal Tansportation problem with quadratic cost with the correct "second boundary value" boundary conditions. It is worth pointing that this has been an open problem for a while. The same paper proposes a fast and robust Newton method (empirically linear) which can be applied to degenerate cases. This potentially means progress in many applications of Optimal Mass Transportation. The method has, for instance, been reimplemented in [72] by TU Eindhoven researchers in collaboration with Philips Lightning Labs to simulate the design of reflectors. In 2013, the method was the topic of invited presentations at the Collège de France applied math seminar, at MSRI (UC Berkeley) special program on Optimal Mass Transportation and at SIAM annual conference on PDE analysis.


../../../../projets/mokaplan/IMG/diff1.png


../../../../projets/mokaplan/IMG/diff5.png

SIERRA Project-Team

2.2. Highlights of the Year

- Visit of Prof. Michael Jordan (U.C. Berkeley) and of his research group.
- Recruitment of two researchers: Alexandre d'Aspremont (DR2 CNRS) and Simon Lacoste-Julien (Inria Starting researcher position).
- Start of a collaboration with Microsoft Research (within the joint MSR/Inria lab).

ANGE Team

2.2. Highlights of the Year

On the one hand, the ERC Consolidator Grant allocated to Anne Mangeney will enable cross-disciplinary works for the modelling of processes governing landslides. In the same spirit, the first Albert Tarantola workshop managed by A. Mangeney and J. Sainte-Marie held on September and aimed at promoting collaborations between mathematicians and geophysicists.

On the other hand, 2013 was dedicated to “Mathematics for Planet Earth” under the patronage of UNESCO. This international initiative consisted in highlighting the role played by mathematics in the modelling of processes that occur on earth including geophysics, biology and human sciences. The ANGE team got involved into this dynamic through the ARP “MathInTerre” from the French agency for research (ANR): scientific committee, organisation of dedicated workshops,...

ARAMIS Team

2.2. Highlights of the Year

Olivier Colliot was invited to give a lecture at the National Academy of Medicine in October 2013.

Stanley Durleman was invited to give a presentation at the Rank Prize Funds symposium "Medical Imaging meets Computer Vision" in March 2013.

BANG Project-Team

2.2. Highlights of the Year

Benoît Perthame was head of the team until January 2013 when he became head of the Laboratoire Jacques-Louis Lions of UPMC (Univ. Paris VI), a laboratory with around 200 members: University, CNRS or Inria permanent members, plus many non-permanents (PhD students, postdocs and engineers). Since then, Marie Doumic has been acting as the BANG team head and now heads the new team MAMBA.

CLIME Project-Team (section vide)

POMDAPI Project-Team (section vide)

REO Project-Team

2.2. Highlights of the Year

- Cristóbal Bertoglio was awarded
  - the best thesis Gamni prize by SMAI.
  - the “Best Thesis in Mathematics and their interactions” prize by the EADS/Airbus Foundation

  for his PhD thesis entitled “Direct and inverse problems in fluid-structure interaction. Application to hemodynamics”, under the supervision of Jean-Frédéric Gerbeau and Miguel Àngel Fernández Varela.
- Justine Fouchet-Incaux, supervised by Céline Grandmont and Bertrand Maury, was awarded the best poster prize by the Société de Physiologie at the 8th congress of "Physiologie, Pharmacologie et Thérapeutique", Anger 2013.

SISYPHE Project-Team

2.2. Highlights of the Year

Results in control of quantum systems obtained by Mazyar Mirrahimi and his former PhD student Zaki Leghtas in close collaboration with the teams of Michel Devoret and Robert Schoelkopf (Department of Applied Physics of Yale University) have been published in *Nature* ([49], [57]) ; *Science* ([47], [60]) ; *Physical Review Letters* ([46], [53]).

ALPINES Team

2.2. Highlights of the Year

- Frédéric Hecht was awarded the EADS Foundation's annual prize for Information Science and its Applications, attributed by the French Academy of Science.
- Best paper finalist at IEEE/ACM Supercomputing 2013 conference, P. Jolivet, F. Hecht, F. Nataf, C. Prud'homme, *Scalable Domain Decomposition Preconditioners For Heterogeneous Elliptic Problems*.
- Best student paper finalist at IEEE/ACM Supercomputing 2013 conference, L. Qu, L. Grigori, F. Nataf, *Parallel Design and Performance of Nested Filtering Factorization Preconditioner*.

ARLES Project-Team

2.2. Highlights of the Year

This year has seen the following acknowledgments of the team's contributions:

PRIZES:

- Valérie Issarny was awarded one of the twelve "Etoiles de l'Europe" for the year 2013. The prize rewards French teams that coordinate European projects as part of the research and innovation framework program, which Valérie received for the FP7 ICT FET CONNECT (Emergent Connectors for Eternal Software-intensive Networked Systems – https://www.connect-forever.eu/) project that examined issues facing the Future Internet.
- Animesh Pathak, Sara Hachem, Giorgios Mathioudakis, and George Rosca were awarded the Best Mashup prize of the OpenDataLab organized by RATP, for their "neverBLate" app.

BEST PAPERS AWARDS :
[12] **REFSQ 2013 - 9th International Working Conference on Requirements Engineering: Foundation for Software Quality**. N. BENCOMO, A. BELAGGOUN.

DYOGENE Project-Team (section vide)

GANG Project-Team (section vide)

HIPERCOM2 Team

2.2. Highlights of the Year

- **PhD Thesis**: Ichrak Amdouni got her PhD Thesis, entitled "Wireless Self-adaptive Ad hoc and Sensor Networks: Energy Efficiency and Spatial Reuse", University Pierre et Marie Curie - Paris VI, February 2013, with Pascale Minet as adviser and Cedric Adjih.
- **PEMWN 2013**: The HIPERCOM2 team actively contributed to the technical and practical organization of the PEMWN 2013 workshop, Performance Evaluation and Modeling of Wireless Networks, held in Hammamet in November 2013. Pascale Minet and Leila Saidane from ENSI (Tunis) were co-general chairs. Cedric Adjih and Paul Muhlethaler were members of the program committee. Christine Anocq was in charge of the pre-registration.
- **Demonstration of OCARI**: The HIPERCOM2 team and more precisely, Cedric Adjih, Ichrak Amdouni, Ines Khoufi, Pascale Minet and Ridha Soua made presentations and demonstrations of the routing protocol and the coloring algorithm of OCARI, an energy-efficient wireless sensor network supporting determinism.

RAP Project-Team (section vide)

REGAL Project-Team

2.2. Highlights of the Year

- Suman Saha received the William C. Carter Award from DSN 2013 . The award recognizes an outstanding paper based on a graduate dissertation, and is the only form of best paper award given at DSN. The award was given for the paper Hector: Detecting Resource-Release Omission Faults in Error-Handling Code for Systems Software.
- Nicolas Geoffray received the 2nd prize for the best PhD thesis in Operating System, from the French Chapter of ACM SIGOPS for his thesis titled “Fostering Systems Research with Managed Runtimes”.
- Inria is the leader of the new European project SyncFree, started in October 2013, described in more detail in Section 7.2.1.1 . SyncFree is based on the CRDT (see Section 5.3.5) and SwiftCloud (Section 4.2) technologies, invented here. CRDTs are data types that are guaranteed to ensure eventual consistency by construction. SwiftCloud is a distributed store that leverages CRDTs to support fast and reliable updates to shared data. This European project, which involves several internet start-ups and academic partners, aims to develop cloud-scale applications that are simpler, more scalable and cheaper.

BEST PAPERS AWARDS :
[44] **DSN 2013 - 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)**. S. SAHA, J.-P. LOZI, G. THOMAS, J. LAWALL, G. MULLER.

ALPAGE Project-Team

2.2. Highlights of the Year

2.2.1. Nomination at the Institut Universitaire de France

Laurence Danlos is a Senior Member of the Institut Universitaire de France since October 2013

2.2.2. Statistical Parsing of Morphologically Rich Languages

Since several years, Djamé Seddah, together with Marie-Hélène Candito and more generally the whole Alpage team, has played a major role in setting up and animating an international network of researchers focusing on parsing morphologically rich languages (MRLs).

This year, Djamé Seddah has led the organization of the **first shared task on parsing MRLs**, hosted by the fourth SPMRL workshop [29]. Its primary goal was to bring forward work on parsing morphologically ambiguous input in both dependency and constituency parsing, and to show the state of the art for MRLs. We compiled data for as many as 9 languages, which represents an immense scientific and technical challenge.

Alpage participated to this shared task with two systems. The first one, applied to French only, belongs to the Bonsai series of parsers, adapted in collaboration with the LIGM in order to better deal with multi-word units [19]. It was **ranked first**, and is therefore the best known parser for French to date.

The other Alpage system which took part to this shared task is Éric Villemonte De La Clergerie's new DyALog-based shift-reduced parser [30], which was applied to all 9 languages. It is the **second best system overall**.

SMIS Project-Team (section vide)

WILLOW Project-Team

2.2. Highlights of the Year

- J. Sivic was awarded a Starting ERC Grant (2014-2018).
- J. Sivic, I. Laptev and J. Ponce (together with C. Schmid, Inria Grenoble) co-organized one week summer school on visual recognition and machine learning http://www.di.ens.fr/willow/events/cvml2013/. The school has attracted 177 participants from 34 countries including Australia, Brazil, Canada, China, Japan, Korea, Russia, Singapore and the United States.

IMARA Project-Team

2.2. Highlights of the Year

- The Grand Prix National de l'Ingénierie 2013 (Grand National Engineering Award 2013 [2]) has been awarded to AKKA Technologies and Inria for the Link & Go project: the first dual-mode concept for an electric vehicle.
- Best paper award for the paper entitled "ABV- A Low Speed Automation Project to Study the Technical Feasibility of Fully Automated Driving" [41] at the workshop on Mobility Assistance and Service Robotics (November 9th, 2013, Kumamoto, Japan).
- Carrefour du PREDIT 2013 Prize: Fawzi Nashashibi was the winner of the Carrefour du PREDIT 2013 for the project SPEEDCAM he coordinated (Speed limit determination using camera and maps). The other partners of this 3-years ANR-DEUFRAKO project are: ARMINES, VALEO, DAIMLER, HOSCHULE AALEN.
- As a member of the Robotics Theme in the field "perception, cognition and interaction" at Inria, IMARA passed successfully the evaluation of the theme organized in March 2013. The evaluation committee was composed of international experts from both academia and industrial backgrounds.

[2] http://www.cgedd.developpement-durable.gouv.fr/le-grand-prix-national-de-l-r159.html