RESEARCH CENTER
Paris - Rocquencourt

FIELD

Activity Report 2015

Section Highlights of the Team

Edition: 2016-03-21

ALPAGE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

In 2015, Alpage has obtained three new national fundings: the team is a partner of two new ANR projects (PARSEME-FR and SoSweet) and an industrial contract ("RAPID" project VeRDI).

5.1.1. Awards

Best Paper Award at the TALN 2015 conference .
BEST PAPERS AWARDS :
[22] **TALN 2015**. M. COAVOUX, B. CRABBÉ.

ALPINES Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. FreeFem++

We have released a version of FreeFem++ (v 3.42) which introduces new and important features related to high performance computing:

- improved interface,
- improved interface with PETSc library,
- improved interface with HPDDM (see above).

This release enables, for the first time, end-users to run the very same code on computers ranging from laptops to clusters and even large scale computers with thousands of computing nodes.

5.1.2. Invited talk Supercomputing 2015

Laura Grigori was an Invited speaker at the ACM/IEEE Supercomputing'15, International Conference for High Performance Computing, Networking, Storage, and Analysis, Austin, November 2015, http://sc15.supercomputing.org/schedule/event_detail?evid=inv103. This is the major conference of high performance computing, attended by 12,000 people. A blog can be found at http://sc15blog.blogspot.com/2015/10/sc15-invited-talk-dr-laura-grigori.html.

5.1.3. SIAM Lecture Note book

Frédéric Nataf, with V. Dolean and P. Jolivet, published a SIAM lecture note book on domain decomposition methods. The four draft versions on HAL https://hal.archives-ouvertes.fr/cel-01100932 were downloaded more than 2 300 times.

5.1.4. SIAM SIAG on Supercomputing

Laura Grigori was elected the Chair of the SIAM SIAG on Supercomputing (SIAM special interest group on supercomputing) for the period of January 2016 - December 2017. She was nominated by a Committee and elected by the members of this SIAG.

ANGE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Contracts and cooperations

- ANR project Hyflo-Eflu accepted
- Industrial contract with SAUR/Agence de l'eau Loire-Bretagne concerning the Vilaine River
- IPL Algae In Silico

Involvment of the team in a large popularisation process

In 2015, members of the team got involved in many popularisation events on behalf of Inria to emphasize the scope of research for the advantages of citizens, whether they be average people, entrepreneurs, decision-makers or students.

ANTIQUE Project-Team (section vide)

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.

ARAMIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Stanley Durrleman has been awarded an ERC Starting Grant by the European Research Council
- The team has been awarded the H2020 project EuroPOND, under societal challenge "Personalizing Health and Care"
- The team has been awarded the ANR-NIH project NETBCI, under the "Collaborative Research in Computational Neuroscience" program (CRCNS)

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.

CLIME Project-Team (section vide)

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.

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).

DYOGENE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Stochastic networks and stochastic geometry conference dedicated to François Baccelli on his 60th birthday

This three day event http://www.di.ens.fr/~blaszczy/FB60/ brought together about twenty invited talks given by leading researchers working on modeling and performance evaluation of computer/communication systems. Mathematical foundations of their work involve, but are not limited to, wireless stochastic geometry, information theory, discrete event dynamical systems, max-plus algebra, stationary-ergodic framework for stochastic networks. It was a wonderful occasion to celebrate the 60th birthday of François Baccelli, who has inspired the development of this field for almost 40 years. The organizers are grateful to all speakers and participants.

Awards

- Ana Busic and Sean Meyn received jointly a Google Faculty Research Award for their research on Distributed Control for Renewable Integration in Smart Communities.
  http://googleresearch.blogspot.com/2015/02/google-faculty-research-awards-winter.html

The Applied Probability Society of INFORMS presents a 2015 Best Publication Award to Mohsen Bayati, Marc Lelarge and Andrea Montanari for their paper

BEST PAPERS AWARDS :

[] **Annals of Applied Probability**. M. BAYATI, M. LELARGE, A. MONTANARI.

EVA Team

5. Highlights of the Year

5.1. Highlights of the Year

Awards

1. **Thomas Watteyne** and Brett Warneke (Linear Technology) received the IPSO CHALLENGE 2015 People's Choice Award with the project "HeadsUp! : Monitoring the Post-surgery Position of Retinal Detachment Patients". 3 December 2015.
2. Danny Hughes, Nelson Matthys, Fan Yang, Wilfried Daniels (KU Leuven, Belgium) and **Thomas Watteyne** received Third Place in the IPSO CHALLENGE 2015, with the project "MicroPnP: Harnessing the Power of IPv6 for Ultra Low Power, Zero-configuration IoT Networks". 2 December 2015.
3. **Thomas Watteyne** elevated to IEEE Senior Member. August 2015.

Meeting & Seminars

TUTORIALS AND KEYNOTES

1. **Keynote** address by **Thomas Watteyne**.
   Nuts and Bolts for Industrial IoT Middleware. ACM/IFIP/USENIX Middleware conference (Middleware), 7-11 December 2015, Vancouver, Canada.
2. **Tutorial** organized by Inria-EVA.
   OpenWSN & OpenMote: Hands-on Tutorial on Open Source Industrial IoT. Thomas Watteyne, Xavier Vilajosana, Pere Tuset. IEEE Global Telecommunications Conference (GLOBECOM), San Diego, CA, USA, 6-10 December 2015.
3. **Tutorial** organized by Inria-EVA.
   OpenWSN Tutorial [presented by Xavi Vilajosana] Workshop Internet Of Things / Equipex FIT IoT-LAB, Lille, France, 15 October 2015.
4. "Demi-heure de la science" presentation by **Thomas Watteyne**.
   Wireless In the Woods: Monitoring the Snow Melt Process in the Sierra Nevada. 3 September 2015, Rocquencourt, France.
5. **Keynote** address by **Thomas Watteyne**.
   The Rise of the Industrial IoT. International Conference on Ad Hoc Networks (AdHocNets), 31 August - 2 September 2015 San Remo, Italy.
6. **Invited Professor Leila Saidane**, from ENSI, Tunisia. She stayed in the EVA team from 18 November to 18 December 2015 to prepare common publications and identify further research directions.

STANDARDIZATION

1. **Standardization** meeting co-chaired by Inria-EVA
   6TiSCH working group meeting at IETF 94, 1-6 November 2015, Yokohama, Japan.
2. **Standardization** meeting co-chaired by Inria-EVA
   6TiSCH working group meeting at IETF 93, 19-24 July 2015, Prague, Czech Republic.
3. **Hackathon** organized by Inria-EVA.
   OpenWSN/6TiSCH Hackathon, Czech Republic, 19 July 2015.
4. **Interop event** organized by ETSI and Inria-EVA
   First ETSI 6TiSCH plugtest (interop event) in Prague, Czech Republic, 17-18 July 2015.
5. **Standardization** meeting co-chaired by Inria-EVA

6TiSCH working group meeting at IETF 92, 22-27 March 2015, Dallas, TX, USA.

ORGANIZATION OF WORKSHOPS AND CONFERENCES

1. **PEMWN 2015** international conference on Performance Evaluation and modeling in Wired and wireless Networks, cochaired by Leila Saidane, **Pascale Minet** and Farouk Kamoun, held in Hammamet, Tunisia, November 2015.
2. **Workshop** organized by Inria-EVA.
   Inria-DGA day on "Software Defined Network (SDN) & MANET" in Paris, October 2015.

INVITED PROFESSORS AND CELEBRATIONS

1. **Pascale Minet** and **Paul Muhlethaler** were invited to celebrate the 30 years of ENSI, Tunisia in November 2015.
2. **Leila Saidane**, professor at ENSI, Tunisia, stayed within the EVA team one month to initiate new common research directions.

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.

GAMMA3 Project-Team

3. Highlights of the Year

3.1. Highlights of the Year

3.1.1. Awards

BEST PAPERS AWARDS :

[] **Procedia Engineering**. A. LOSEILLE, V. MENIER, F. ALAUZET.

GANG Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Roads

COMPUTATION OF ROAD NETWORK DIAMETER

Based on the algorithms presented in [5], Laurent Viennot has computed the diameter and radius of the worldwide road network. The diameter of a graph is the distance between two points that are furthest apart one from another. The interesting distance notion in a road network is often travel time. Finding the worldwide road network diameter thus amounts to find two points such that the travel time from one to another is maximal. Once such a pair of points is identified, we can compute the shortest path between them to obtain somehow the longest road trip in the world. Computing the diameter of a general graph usually requires to compute all pairwise distances, which is impractical for such a big graph. However, the team has developed heuristics that appear to work fast on many practical graphs including road networks. Thanks to OpenStreetMap data, the team has thus been able to compute the world road diameter (and the diameter of various restricted parts of the network). The results can be visualized on https://who.rocq.inria.fr/Laurent.Viennot/road/.

Erc

NEW ERC CONSOLIDATOR GRANT

Amos Korman has received an ERC Consolidator Grant, entitled “Distributed Biological Algorithms (DBA)”, which started in May 2015. The goal of this interdisciplinary project is to demonstrate the usefulness of an algorithmic perspective in studies of complex biological systems. It focuses on the aspect of collective behavior, demonstrating the benefits of applying distributed computing techniques to establish algorithmic insights into the behavior of biological ensembles.

Highpapers

WORK ON DISTRIBUTED COMPUTING

The team has published a number of papers on Distributed Computing theory at high-profile venues. A subjective selection of these results includes: an almost-tight bound on the space complexity of set agreement [29], a study of the power of randomization in proof-labeling schemes [22] (both published at PODC’15), and a characterization of convergence in an important class of population protocols [28] (published at ICALP’15 track A).

LIFEWARE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Four PhD Theses Defended this Year

Katherine Chiang defended her thesis [1] in three years at National Taiwan University and two internships with us in 2012 and 2013, on the computer-aided design of biomolecular systems, a subject co-supervised by Jie-Hong Jiang and François Fages which is of increasing importance in Lifeware and led to several publications this year [11], [6], [5].

Artemis Llamosi defended his thesis [3] in three years also, on the modeling of cell-to-cell variability, a subject co-supervised by Grégory Batt and Pascal Hersen, which led to a major publication in *PLoS Computational Biology* [8] to appear in 2016, and a cooperation with Marc Lavielle (EP POPIX).

Steven Gay finally defended his thesis [2] on subgraph epimorphisms and model reductions, a subject co-supervised by François Fages and Sylvain Soliman, 18 months after he leaved us for taking a Post Doc position at Univ. Louvain-la-Neuve, Belgium.

Thierry Martinez defended his thesis [4] supervised by François Fages, on a logical kernel for constraint programming, with direct impact on the design of the ClpZinc modeling language and the rewriting of Biocham v4, for which he got engineer positions n the last years.

In addition, François Bertaux has sent to reviewers his thesis on the modeling of cell-to-cell variability and cell apoptosis, co-supervised by Dirk Draso and Grégory Batt. Sylvain Soliman has sent to reviewers his *Habilitation à Diriger des Recherches* on the dynamics of biochemical systems. Pauline Traynard is also finishing her thesis co-supervised by François Fages and Denis Thieffry, on temporal logic patterns and solvers and the modeling of the interactions between the cell cycle and the circadian clock, for a defense in early 2016 in three years and half. Jean-Baptiste Lugagne is also expected to defend his thesis in 2016.

These theses are the foundations of some major themes of Lifeware for the next years.

MAMBA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Awards

Benoît Perthame is the 2015 laureate of the Inria - French Académie des Sciences Grand Prize: http://www.inria.fr/en/institute/inria-in-brief/inria-awards/2015-prize-winners/benoit-perthame-grand-prize.

MATHERIALS Project-Team (section vide)

MATHRISK Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Conference in honor of Vlad Bally for his 60th birthday, Le Mans, October 6-9 2015 http://www.cmap.polytechnique.fr/~demarco/files/pageWebConfV/ConferenceVladBally.html

5.1.1. Awards

J. Reygner received the 2014 Jacques Neveu prize for his thesis entitled "Longtime behaviour of particle systems : applications in physics, finance and PDEs" co-supervised by B.Jourdain and L. Zambotti

MIMOVE Team

5. Highlights of the Year

5.1. Highlights of the Year

On Wednesday July 8, 2015, Inria announced the launch of SoundCity, a mobile application to measure your personal exposure to noise pollution. The project is developed in the context of CityLab@Inria by the MiMove and CLIME teams, further involving collaboration with French and California startups. The project is supported by the City of Paris smart city initiative and Bernard Jomier, deputy mayor responsible for health, disability, and relations with Paris public hospital system. Noise pollution, which lowers quality of life and harms health, is a serious environmental challenge in almost every major city. The noise levels found in most cities today can interfere with memory and learning, disturb sleep, and contribute to heart disease. In Paris, the urban ecology agency and the Bruitparif association [0] currently rely on monitoring stations and computer simulations to understand noise exposure of citizens. SoundCity aims to complement these data with personal sound level exposure measurements collected with smartphones. SoundCity will also help citizens be more aware and engaged with noise in their environments. More at http://www.inria.fr/en/centre/paris/news/launch-of-soundcity-mobile-application.

[0] http://www.bruitparif.fr

MOKAPLAN Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Fast entropic methods for optimal transport problems: In a series of papers [19] [34] [10] [15] , MOKAPLAN's team members derived a new class of algorithm to obtain efficient approximations of the solution to various problems related to OT (including barycenters, Euler equation, unbalanced problems, gradient flows). This method makes use of entropic regularization and first order optimization method for the Kullback-Leibler divergence. See Section 6.3 for details about the software output.

Relaxing the mass conservation constraints: Our team derived a new theoretical and numerical framework to deal with "unbalanced" optimal transport problems [38], [39]. This contribution is a breakthrough that will open the door to application in image processing and machine learning. See Section 7.6 for more details.

MUSE Team (section vide)

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.

MYCENAE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- HDR defense of Jonathan Touboul : Contribution to the theoretical study of large neuronal ensembles. June 5th 2015, ED3C
- Co-organization of founding events to federate the national scientific communities in Reproduction: Reprosciences 2015, and in Modeling for cell and developmental biology: 2015 ITMO BCDE workshop on Modeling in Cell and Developmental Biology

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.

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.

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.

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

QUANTIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- First demonstration of Quantum Zeno Dynamics of light: this important experimental result offers a new scheme to control quantum systems based on light modes and was published in Science in 2015 [13].
- In a collaboration with the team of Michel H. Devoret at Yale university, we engineered a new form of quantum friction. By engineering a particular non-linear interaction between a quantum harmonic oscillator (a superconducting cavity mode) and a driven bath, we were able to stabilize a manifold of quantum states. This result which was published in Science in 2015 [18] should lead to a new direction of research in quantum information processing with driven dissipative systems.
- In a collaboration with the team of Robert J. Schoelkopf at Yale university, we were able to realize a version of Schrdoinger's cat thought experiment. We were able to entangle an artificial atom to a cat state of a quantum harmonic oscillator. We were able to characterize this entanglement using the Clauser-Horne-Shimony-Holt formulation of a Bell test. This result was published in Nature Communications [25].

RAP Project-Team (section vide)

REGAL Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

- *Garbage collection for big data on large-memory NUMA machines*. We developed NumaGiC, a high-throughput garbage collector for big-data algorithms running on large-memory NUMA machines. This result, a collaboration with the Whisper team, has been presented at ASPLOS 2015 [49].
- *Explicit consistency*. We propose an alternative approach to the strong-vs.-weak consistency conundrum, *explicit consistency*. This result has been presented at EuroSys 2015 [80]. We have also developed a new sound logic for proving the correctness of a distributed database under concurrent updates. This result is published at POPL 2016 [50].
- *The weakest failure detector of implement eventual consistency*. We found the weakest failure detector to implement an eventually consistent replicated service. This theoretical result has been presented at PODC 2015 [46].

4.1.1. Awards

Gauthier Voron obtained best paper award at system track of Compas'2015.
BEST PAPERS AWARDS :
[64] **Conférence en Parallélisme, Architecture et Système, (COMPAS'15)**. V. GAUTHIER, G. THOMAS, P. SENS, V. QUEMA.

REO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

Irène Vignon-Clementel: Article [16] selected for journal cover in Cardiovascular Engineering and Technology.

5.1.1. Awards

Jessica Oakes was awarded an American Lung Association Senior Research Training Grant for salary support for 1-2 years.

RITS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Fawzi Nashashibi was awarded by the Higher Council for Innovation & Excellence in Palestine for his innovation research on intelligent transportation. The award was delivered by President Mahmoud ABBAS at the 1st HCIE National Forum for Innovators on innovation, September 12-13 2015, Ramallah, Palestine.

BEST PAPERS AWARDS :

[30] **ITS World Congress 2015**. A. DE LA FORTELLE, X. QIAN.

[35] **2015 IEEE International Conference on Vehicular Electronics and Safety**. R. LUIS, J. PÉREZ RASTELLI, D. GONZALEZ BAUTISTA, V. MILANÉS.

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.

SERENA Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Martin Vohralík obtained the ERC consolidator grant in the 2015 campaign with his project GATIPOR “Guaranteed fully adaptive algorithms with tailored inexact solvers for complex porous media flows”.

Jérôme Jaffré was awarded the 2015 SIAM Geosciences Senior Career Prize.

SIERRA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

F. Bach has served as a program co-chair for the International Conference in Machine Learning (ICML) held in Lille, France, 2015.

SMIS Project-Team (section vide)

WHISPER Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The main highlight of the year is the continuous spreading of Coccinelle within the developer community of the Linux kernel. We submitted the first patches to the Linux kernel based on Coccinelle in 2007. Since then, over 4500 patches have been accepted into the Linux kernel based on the use of Coccinelle, including around 3000 by over 500 developers from outside our research group. Another testimonial of the impact of our work is the visit of Greg Kroah-Hartman in March and April 2015, as an Inria invited researcher. Kroah-Hartman is one of the leading developers of the Linux kernel, and at the time only one of two developers employed by the Linux Foundation, with the other being Linus Torvalds. Greg participated in the activities of the Whisper team around the use of Coccinelle and research projects related to the Linux kernel, and he is a convinced ambassador of our research work.

Our work on Remote Core Locking (RCL) [10] was accepted in ACM Transaction in Computer Systems (TOCS) which is the most prestigious journal in systems. RCL is currently one of the most efficient locks for multicore architectures.

WILLOW Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

J. Sivic has served as a Program Chair for International Conference on Computer Vision, Santiago, Chile, 2015