RESEARCH CENTER
Paris

FIELD

Activity Report 2017

Section Highlights of the Team

Edition: 2018-02-19

ANTIQUE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The team obtained several strong results published in excellent international conferences, with high theoretical and applied impact (see detailed results). Among the theoretical results we underline those presented in conferences like Principles of programming languages POPL 2017, with the proposal of a novel and groundbreaking way to improve the precision and scalability of analyses performed with disjunctive abstract domains, using silhouette abstraction.

5.1.1. Awards

Patrick Cousot received the IEEE John Von Neumann Medal.

AOSTE2 Team

5. Highlights of the Year

5.1. Highlights of the Year

Our team has hosted for the first time in France the 38th Real-Time Systems Symposium (RTSS'17) which is the flag conference of our research domain. All the members of team jointly participated to the big effort of ensuring an excellent edition.

CASCADE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Conferences

- We organised the Eurocrypt '17 annual conference in Paris, from April 30 to May 4.

5.1.2. Awards

- Damien Vergnaud was nominated for a 5 year appointment as Junior Member of the Institut Universitaire de France
- Romain Gay received a Google PhD Fellowship.

GALLIUM Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

In 2017, Jacques-Henri Jourdan received the “prix du GDR GPL” (http://gdr-gpl.cnrs.fr/node/284) for his dissertation, entitled “Verasco: a Formally Verified C Static Analyzer”. Jacques-Henri was a Ph.D. student in the Gallium team, advised by Xavier Leroy.

PARKAS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

- Francesco Zappa Nardelli received the *Most Influential ICFP Paper Award* for 2007 paper "Ott: Effective Tool Support for the Working Semanticist" (http://www.sigplan.org/Awards/ICFP/).

PI.R2 Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Amina Doumane was awarded the The Kleene Award for Best Student Paper at the LICS 2017 conference, for her work on “Constructive Completeness for the Linear-Time mu-Calculus”. She also received in January 2018 the prize of the Journal La Recherche for the same paper.

Amina Doumane was awarded the Gilles Kahn 2017 prize for her PhD thesis entitled “On the infinitary proof theory of logics with fixed points” supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien.

Ludovic Patey was awarded the Prix Thiessé de Rosemont / Demassieux 2017 for his PhD thesis “Les mathématiques à rebours de théorèmes de type Ramsey”, supervised by Laurent Bienvenu and Hugo Herbelin.
BEST PAPERS AWARDS :
[37] **Conference on Logic in Computer Science 2017**. A. DOUMANE.
[] **On the infinitary proof theory of logics with fixed points**.

POLSYS Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

Dongming Wang has been elected as a Member of the Academia Europaea.

Elias Tsigaridas was awarded an ANR “Jeune Chercheur Grant”. The title of the project is GALOP (Games through the lens of ALgebra and OPptimization)

PROSECCO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- We published 20 papers at top-tier conferences such as POPL (2), IEEE S&P (2), ACM CCS (1), IEEE CSF (1), ICFP (1), PETS (1), and IEEE Euro S&P (2).
- Bruno Blanchet published a paper on the applied pi calculus in the prestigious Journal of the ACM.
- The HACL* verified cryptographic library developed in our group was integrated into Mozilla Firefox 57 and is being actively used by hundreds of millions of users around the world.
- We organized the second edition of the IEEE Euro S&P Conference in Paris, which was attended by over 200 security researchers from around the world.

5.1.1. Awards

- Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi won a Distinguished Paper award at IEEE S&P 2017 .
- Catalin Hritcu was awarded a new DARPA SSITH grant called HOPE with DRAPER Labs.
- Antoine Delignat-Lavaud received an “accessit” for the prix de thèse GDR GPL 2016.

BEST PAPERS AWARDS :
[24] **38th IEEE Symposium on Security and Privacy**. K. BHARGAVAN, B. BLANCHET, N. KOBEISSI.

SECRET Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. NIST post-quantum cryptography standardisation

The end of this year was the deadline to submit proposals to the NIST competition [0], whose purpose is to standardize quantum-safe public-key primitives. This call concerns all three major cryptographic primitives, namely public-key cryptosytems, key-exchange protocols and digital signature schemes. The most promising techniques today for addressing this issue are code-based cryptography, lattice-based cryptography, mutivariate cryptography, and hash-based cryptography.

We have contributed to three proposals to the NIST call. In two of them, "BIKE" [67] and "Big Quake" [69], our action is central and we also have a marginal participation in another, "Classic McEliece". Those projects are of great importance for us because they are a means to demonstrate our long lasting expertise in code-based cryptography. They are the product of numerous research works, including several PhD theses, on the design, the implementation, and the cryptanalysis of code-based cryptographic primitives. There are 69 projects in that call, which will be evaluated by the NIST and the academic cryptographic community in the next three to five years and whose outcome will certainly influence cryptographic applications for one or several decades.

5.1.2. Quantum symmetric cryptanalysis and collision search

The resistance of symmetric primitives to quantum computers is a topic that has received recently a lot of attention from our community. The ERC starting grant QUASYModo on this subject, awarded to M. Naya-Plasencia, has started in September 2017. We have continued the work started last year obtaining new results, as cryptanalysis of concrete proposals [44], or analysis on attacks considering modular additions (preliminary described in [14]). In particular, we have proposed in [47] a new quantum algorithm for finding collisions. This new algorithm, based on BHT, exploits distinguished points as well as an improved optimization of the parameters, and allows to find for the first time, collisions on n bits with a better time complexity than $2^{n/2}$. Its time and query complexity are of about $2^{2n/5}$, needing $2^{n/5}$ classical memory and a polynomial amount of quantum memory. As collision search is a tool widely used in symmetric cryptanalysis, this algorithm, that also can be applied to multiple preimage search, considerably improves the best known previous attacks when having a relatively small quantum computer available.

5.1.3. Émergences grant on quantum money

André Chailloux was awarded an Émergences grant from the city of Paris for a project on quantum money. This project aims at providing a comprehensive theoretical and experimental study of unforgeable quantum money, one of the most powerful protocols in quantum information science, and historically the first. A quantum money scheme enables a secure transaction between a client, a vendor and a bank via the use of a credit card or banknotes, with maximal security guarantees, unreachable with classical technologies. This application is central in the context of the emerging quantum network infrastructures guaranteeing the long-term security of data and communications against all-powerful adversaries.

Quantum money has been largely considered difficult to bring to the experimental realm, but a demonstration became more accessible recently, thanks to the conception of new practical schemes. The goal of our project will be to perform a theoretical analysis of such schemes, both in the discrete and continuous-variable frameworks, to adapt them to realistic conditions, and to implement them using state-of-the-art photonic quantum technologies. The project, centered around Inria, is interdisciplinary at its core, bringing together young partners with world leading expertise in all aspects of the proposed work, including theoretical and experimental quantum cryptography.

[0] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

MATHERIALS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

E. Cancès was awarded the 2017 Dargelos Prize from the Alumni of Ecole Polytechnique.

MATHRISK Project-Team (section vide)

MOKAPLAN Project-Team (section vide)

QUANTIC Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Rémi Azouit (supervisor: Pierre Rouchon; co-supervisor: Alain Sarlette) has successfully defended his PhD thesis on October 27th and is now moving as a postdoc to Sherbrooke University. This thesis provides a systematic approach towards model reduction through adiabatic elimination for open quantum systems.
- Joachim Cohen (supervisor: Mazyar Mirrahimi) has successfully defended his PhD thesis on February 2nd. This thesis provides a roadmap for future experiments on autonomous hardware efficient quantum error correction with superconducting circuits.

5.1.1. Awards

- Mazyar Mirrahimi has received the “Inria-Academie des Sciences young researcher award 2017”.
- Pierre Rouchon has received the “Grand Prix IMT-Academie ses Sciences 2017”.

SIERRA Project-Team (section vide)

ANGE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Human resources

A major event in the year was the merging with CLIME which induces the incorporation of several new researchers (1 Researcher, 1 engineer, 2 PhD). CLIME research is naturally complementary to ANGE works insofar as it provides high level tools to improve modelling and numerical results.

Another fact is J. Salomon's arrival as a Senior Researcher.

5.1.2. Scientific activities

There has been major achievements within the team in the framework of dispersive models. An increased research activity is carried out with spanish collaborators (Univ. Sevilla, Córdoba and Málaga) supported by several project call fundings. This lead to a main publication [30]. In the aftermath of N. Aïssiouene's PhD thesis, a new PhD has been hired to go further in the design of robust and efficient numerical algorithms.

As detailed in Section 10.1.1.1 , members of the team were involved in the organisation of a substantial number of scientific events, either in the framework of national initiatives (mainly funded by CNRS) or due to the expertise in the field. Members are is particularly involved in the mathematical community.

5.1.3. Awards

L. Boittin and F. Wahl were granted a SIAM Student Travel Award to attend SIAM GS 2017. F. Wahl also received a Young Researcher Scholarship to attend the 2017 SMAI conference.

ARAMIS Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- Anne Bertrand spent a year half-time within the ARAMIS team, thanks to an Inria-APHP interface contract (i.e., "poste d'accueil"), from november 2016 to november 2017. At the end of this contract, she was appointed as an Assistant Professor of Radiology at Sorbonne University, on september 2017, allowing her to continue working 40% of her time within the ARAMIS team.
- Fabrizio De Vico Fallani was named associate editor of the journal Brain Topography
- Stanley Durrleman was nominated coordinator of the ICM Center of Neuroinformatics, and scientific manager of the ICM iCONICS core-facility on bioinformatics.
- The team has been awarded the projects SEMAPHORE, ATTACK and PredictICD under the "Big Brain Theory" program (ICM)

5.1.1. Awards

- Jeremy Guillon was awarded the best lighting presentation at the international conference on complex networks

MAMBA Project-Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Benoît Perthame has been elected member of the Académie des Sciences, in the section “Physique, mécanique, informatique”.

4.1.2. Personnel

Marie Doumic has prolonged for one more year her sabbatical at WPI (Vienna, Austria, 2016-2018).

Diane Peurichard has been hired as Chargée de Recherche classe normale in Mamba, beginning in October 2017.

MYCENAE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

- We have completed in [17] our series of studies [8], [12], [6], [2], [4], [3] on the mathematical and numerical analysis of our multiscale model of structured cell populations in terminally developing ovarian follicles.
- We have completed in [19] our series of studies [27], [26], [35], [29], [32] on the mathematical and numerical analysis of our model of GnRH pulse and surge generator.

REO Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

Mikel Landajuela Larma was awarded the 2017 SMAI-GAMNI PhD thesis prize by the French Society of Industrial and Applied Mathematics for his thesis supervised by Miguel Fernández.

SERENA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

The most important results of the ERC GATIPOR are now centralized in the ERC GATIPOR Gallery.

5.1.1. Awards

Laurent Monasse was awarded an ANR JCJC (young researcher) grant.

TAPDANCE Team

4. Highlights of the Year

4.1. Highlights of the Year

4.1.1. Awards

Tristan Stérin won a best poster award at the conference DNA 23.

ALPINES Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards and Recognitions

5.1.1.1. Laura Grigori elected Member of the SIAM Council

January 2018 - December 2020.

DYOGENE Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

B. Blaszczyszyn has just been appointed ENS adjunct professor in September 2017.

EVA Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

1. **Pascale Minet**, **Paul Muhlethaler** and Ines Khoufi received the best paper award for their paper "Coded Slotted Avoidance in a Wireless Network: Models and Simulations" at PEMWN 2017.
2. SolSystem selected as one of the 10 testbeds at the IoT Solutions World Congress, Barcelona, Spain, 3-5 October 2017.
3. SmartMesh IP awarded "Internet of Things Product of the Year" at the Annual Creativity in Electronics (ACE) Awards, 6 December 2017. (Note: this is not a personal award)

5.1.2. 6TiSCH Standardization Virtually Completed

Time Synchronized Channel Hopping (TSCH) is a Medium-Access Control (MAC) technique in which nodes synchronize, and a schedule orchestrates all communication in the network. Inria-EVA created the IETF 6TiSCH Working Group in 2013. The goal of 6TiSCH is to get the best of both world by combining TSCH ("industrial" performance) and the ease of use of IPv6 through the IETF upper stack (6LoWPAN, RPL, CoAP). Since the creation of 6TiSCH in October 2013, **Thomas Watteyne** co-chairs the working group, helps drive its technical developments, and coaches authors and authors technical documents. 6TiSCH also encompasses and important security aspect, where we look how to enable nodes to join a network efficiently, which includes mutual authentication between node and network. The 6TiSCH security solution if based on PSK, and relies on AES-128 CCM*.

421 people now follow the 6TiSCH activities through its mailing-list, with a healthy mix of industrial and academic contributors. In 2017, 6TiSCH has produced 2 RFCs, 6 working group document in the process of being published, and various individual submissions. The working group has met 3 times in person during 2017, tens of times through Webex. Inria-EVA co-organized a 6TiSCH interop event (attended by 15 entities) in July 2017. 6TiSCH is now supported by all major open-source implementations (OpenWSN , Contiki , RIOT, TinyOS), and several companies are building commercial product lines with it. 6TiSCH has been playing a real role of catalyst for the academic low-power wireless community, which has now mostly moved towards TSCH/6TiSCH.

5.1.3. Over 1,000 Sensors Deployed on 3 Continents

Inria-EVA uses SmartMesh IP as a low-power wireless building block for building end-to-end solutions. Deploying real networks allows Inria-EVA to do system-level cross-disciplinary research. Inria-EVA oversees over 1,000 sensors deployed on 3 continents:

- http://snowhow.io/. Monitoring the snowmelt process in the California Sierra Nevada. 945 sensors deployed in 21 networks. Collaboration with UC Berkeley Prof. Steven Glaser.
- http://www.savethepeaches.com/. Predicting frost events in peach orchards. 120 sensors deployed in Mendoza, Argentina. Collaboration with local agronomy/networking teams
- http://smartmarina.org/. Monitoring the occupancy and per-boat water/electricity consumption of the 3rd largest marina in Europe (Cap d'Agde, 4300 boats). Inria-EVA is working on turning this activity into a startup company.

GANG Project-Team (section vide)

MIMOVE Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- R. Teixeira was selected to appear in the 2017 list of "N2Women: Stars in Computer Networking and Communications".
- The AppCivist project, which is a joint initiative between the Social Apps Lab at UC Berkeley and the MiMove team at Inria, won the 2016-17 Chancellor's Award for Public Service in the category of Campus-Community Partnership in collaboration with the City of Vallejo [20].

BEST PAPERS AWARDS :
[19] **IEEE International Conference on Collaboration and Internet Computing**. R. ANGARITA, N. GEORGANTAS, V. ISSARNY.

RAP2 Team (section vide)

REGAL Project-Team (section vide)

WHISPER Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

As part of a collaborative effort with Timothy Bourke, Lélio Brun, Marc Pouzet (Parkas team), Xavier Leroy (Gallium team), Lionel Rieg (Collège de France) and Pierre-Évariste Dagand, our work on a certified Lustre compiler was accepted at PLDI [13].

Julia Lawall was invited to present a talk as part of the Colloquium Jacques Morgenstern at Inria - Sophia Antipolis. The talk was entitled "Coccinelle: synergy between programming language research and the Linux kernel". A video of the presentation is available. [0]

The work of Julia Lawall on the Linux kernel was featured in the Linux Foundation's 2017 Linux Kernel Development Report. [0]

[0] https://www.canal-u.tv/video/inria/coccinelle_synergy_between_programming_language_research_and_the_linux_kernel.38185
[0] https://www.linuxfoundation.org/2017-linux-kernel-report-landing-page

ALMANACH Team

5. Highlights of the Year

5.1. Highlights of the Year

- ALMAnaCH's submission to the 2017 CoNLL multilingual parsing shared task was ranked 3rd (out of 33) in part-of-speech tagging, and 6th (out of 33) in dependency parsing.
- Joint submissions of ALMAnaCH and Stanford University to the Extrinsic Parsing Evaluation campaign ranked 1st and 3rd.

COML Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

BEST PAPERS AWARDS :
[67] **Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)**. B. LUDUSAN, R. MAZUKA, M. BERNARD, A. CRISTIA, E. DUPOUX.

RITS Project-Team (section vide)

Valda Team (section vide)

WILLOW Project-Team

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. Awards

- J. Sivic (together with J. Philbin, O. Chum, M. Isard, and A. Zisserman) received the Longuet-Higgins Prize for "Fundamental contributions in Computer Vision", awarded at the IEEE Conference on Computer Vision and Pattern Recognition, 2017.
- J. Sivic (together with A. Zisserman) received the Helmholtz Prize for "fundamental contributions to computer vision", awarded at the International Conference on Computer Vision, 2017.
- J. Sivic (together with B. Russell, A. Efros, B. Freeman and A. Zisserman) received the Helmholtz Prize for "fundamental contributions to computer vision", awarded at the International Conference on Computer Vision, 2017.
- I. Laptev (together with T. Lindeberg) received the Helmholtz Prize for "fundamental contributions to computer vision", awarded at the International Conference on Computer Vision, 2017.