RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2016

Section Popularization

Edition: 2017-08-25

ARIC Project-Team

9.3. Popularization

Claude-Pierre Jeannerod gave an invited talk at *Journés Nationales de l'APMEP* (Lyon, October 2016), on the theme of algorithms for computer arithmetic.

Paolo Montuschi (Politecnico di Torino) and Jean-Michel Muller wrote a short paper on Computer Arithmetic for Computer Magazine [51].

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l'Informatique, and in particular she was involved in the creation of the *Magimatique* exhibition. She presented some magic tricks during *Forum des Associations de Lyon 7e* and during the Science Fair, and she helped a class of high-school pupils (2nd) of Lycée Juliette Récamier (Lyon) to prepare a show for other pupils. She belonged to the selection committee for the MathInfoLy summer school for high-school pupils (around 90 french-speaking pupils). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Lucie Aubrac (Ceyzériat), Lycée Xavier Bichat (Nantua) and Mondial des Métiers (in January and February 2016). She presented computer science for primary school pupils (CM2, École Guilloux, St-Genis-Laval: 12 lectures and hands-on of 1h30 in 2015-2016, for each of the 2 classes). She presented this work during the *Journées Passeurs de Science Informatique* of SIF in June 2016 and during the workshop *Robots pour l'éducation*. She also presented this work at a TEDxINSA talk and for IESF (Ingénieurs et Scientifiques de France). She took part in a training session for teachers, sponsored by Google, in September 2016. She co-organized two days on "Info Sans Ordinateur" gathering researchers interested in unplugged activities. With Jérôme Germoni and Natacha Portier, she co-organized a day *Filles & Maths* in May 2016 and a day *Filles & Info* in November 2016, each gathering about 100 high-school girls of 1e S. She is one of the editors of Interstices: https://interstices.info. She taught how to disseminate (computer) science for PhD students in a 20h module of *Insertion Professionnelle*.

Damien Stehlé will give a talk at the CNRS 'Colloque Sociétal Sécurité Informatique' (December 2016), on Fully Homomorphic Encryption.

AROMATH Project-Team (section vide)

10.3. Popularization

- Laurent Grémy and Pierre-Jean Spaenlehauer have animated a stand in the “Village des Sciences du Loria” in March 2016.
- Laurent Grémy and Pierre-Jean Spaenlehauer have animated a stand during the celebration of the Loria’s 40 years anniversary in June 2016.
- Pierrick Gaudry organized and participated to a debate fed by excerpts from movies on the topic of cryptography and privacy in October 2016.

CASCADE Project-Team (section vide)

DATASHAPE Team (section vide)

GRACE Project-Team

10.3. Popularization

- At the occasion of Nokia Bell Labs Future X-Days, September 2016, D. Augot, N. Coxon and F. Levy-dit-Vehel demoed N. Coxon's implementation of a code based *private information retrieval scheme*
- D. Augot made a two hours lecture on bitcoin to the French *institut des actuaires*.

LFANT Project-Team

8.3. Popularization

D. Robert wrote with Sorina Ionica the chapter "Pairings" of the book Guide to Pairing-Based Cryptography [16] which will be published by CHAPMAN and HALL/CRC. This book aims to help Engineers understand and implement pairing based cryptography. In the Chapter Pairings D. Robert give a self contained definition and proof of the Weil and Tate pairing; including how to handle divisors with non disjoint support (this is often skipped in scientific papers but is important for practical implementations).

H. Cohen wrote a vulgarisation article [17] on Fermat's last theorem. This article explain (through the example of congruent numbers) the role of elliptic curves and algebraic number theory in the solution of Fermat's last theorem.

During the last PARIatelier four talks [19], [18], [20], [21] have been filmed and are available under a creative common licence. This will allow people from all the world to get started faster with PARI. The first two talks focus on setting up personal computers for the atelier and the new features of PARI. The next two are more technical and explain the new L-functions and modular forms features.

9.3. Popularization

J.-C. Faugère and L. Perret wrote a paper “Le grand défi du post-quantique” for MISC (HS 13, April 2016).

SECRET Project-Team

10.3. Popularization

- Nicolas Sendrier and Jean-Pierre Tillich, *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, ERCIM News [67].
- Anne Canteaut gave a talk at the *dotSecurity 2016* conference for developers, at Théâtre des Variétés, Paris, April 2016 http://www.thedotpost.com/2016/05/anne-canteaut-the-struggle-for-secure-cryptography.
- Anne Canteaut gave a talk at *Séminaire général du département d'informatique de l'ENS* for Master students in computer science at ENS Paris, April 13, 2016 http://savoirs.ens.fr/expose.php?id=2516.
- André Chailloux gave a talk entitled *L'ordinateur quantique*, at Journées Art, Cerveau, Futur; Mouans-Sartoux, France, September 2016;
- Anne Canteaut gave a talk on cryptography at lycée Rodin, Paris, February 2, 2016.
- Sébastien Duval gave a talk on cryptography at lycée des 7 Mares, Maurepas, December 2, 2016
- Anne Canteaut has been involved in the AlKindi competition, which is a national competition on cryptanalysis for students in "Seconde" http://www.concours-alkindi.fr/.

  The best teams from Paris have been visiting the SECRET project-team in June 2016 https://www.youtube.com/watch?v=EVLHEOWAORc.
- Julia Chaulet participated to a general-public mediation about the use of mathematics in industry at "Salon Culture & Jeux Mathématiques", Paris, May 28, 2016.
- Yann Rotella hold a stand to explain cryptography at Futur en Seine, Carreau du Temple, Paris, June 12, 2016.

SPECFUN Project-Team

9.3. Popularization

- Assia Mahboubi has written a paper [8] for the quarterly journal of the Royal Dutch Mathematical Society.
- Alin Bostan has given a talk at the *Mathematic Park* seminar at IHP, Paris, on January 23rd 2016.

VEGAS Project-Team (section vide)

CAIRN Project-Team (section vide)

CAMUS Team

10.3. Popularization

Jens Gustedt is regularly blogging about efficient programming, in particular about the C programming language. He also is an active member of the stackoverflow community a technical Q&A site for programming and related subjects. A first complete online version of his book *Modern C*, to appear in 2017, has been accessed more than 10000 times on a single day.

COMPSYS Team

10.3. Popularization

The interdisciplinary spring school organized in May 2016 (see Section 10.1) is a form of popularization of compiler technology (in particular polyhedral optimizations) towards HPC users from the numerical simulation community.

CORSE Project-Team (section vide)

DREAMPAL Project-Team (section vide)

PACAP Project-Team

10.3. Popularization

Erven Rohou discussed the research axes of the team in the “émergences” newsletter http://emergences.inria.fr/2016/newsletter_n43/L42-PACAP.

Nicolas Kiss, Damien Hardy and Erven Rohou presented a poster at the “Rencontres inter-UMRs-DGA”, of the “Pôle d’excellence Cyber”.

Erven Rohou and Isabelle Puaut presented a poster (with ANR W-SEPT colleagues) at “Les rencontres du numérique de l’ANR”.

TASC Project-Team

10.3. Popularization

- Maintenance of the global constraint catalogue.
- Illustrations of the volume II of the global constraint catalogue: 2000 figures.

AOSTE Project-Team

9.3. Popularization

Liliana Cucu-Grosjean has supervised the video production of a popularization video regarding the outcomes of the PROXIMA project. The video has been made available on Inria channels and all PROXIMA partners.

CONVECS Project-Team

9.3. Popularization

H. Garavel participates to the program committee and organization committee of FMF (Formal Methods Forum [0]), a series of industrial conferences on formal methods set up by the competitivity clusters Aerospace Valley and Minalogic, with the support of Inria and many other partners. The 6th FMF conference, devoted to safety engineering, was held on January 26, 2016. The 7th FMF conference, devoted to formal methods and cybersecurity, is scheduled on January 31, 2017.

H. Garavel and R. Mateescu co-operated with Gérard Berry to prepare his lecture on explicit-state enumerative verification given at Collège de France on April 22, 2016.

[0] http://projects.laas.fr/IFSE/FMF

HYCOMES Project-Team (section vide)

MUTANT Project-Team (section vide)

PARKAS Project-Team (section vide)

POSET Team

10.3. Popularization

The development of the T-calculus has eventually led us to a piano & computer performance that is going to be performed on stage in February 2017 with the pianist Edwin Bugger, associate member of the PoSET project.

SPADES Project-Team

9.3. Popularization

Alain Girault gave a lecture to high school math professors, titled “Multi-core architectures, reliability, and optimization” (ISN conference cycle, Grenoble, February 2016). http://www.canal-u.tv/video/inria/architectures_multi_coeurs_ fiabilite_et_optimisation.20829

TEA Project-Team (section vide)

ANTIQUE Project-Team (section vide)

CELTIQUE Project-Team

6.3. Popularization

Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, given three times in high schools close to Rennes.

DEDUCTEAM Team (section vide)

GALLIUM Project-Team

10.3. Popularization

Xavier Leroy gave a popularization talk on formal methods at the plenary days of Inria's DGD-T (may 2016) and another on critical avionics software for first-year students at École Polytechnique (june 2016).

MARELLE Project-Team

7.3. Popularization

Laurent Théry gave talks in the context of “Fête de la science”.

MEXICO Project-Team

9.3. Popularization

- Stefan Haar gave a talk entitled 'Post hoc sed non propter hoc, or: why you should care about causality', in the Seminar@SystemX series of IRT SystemX on September 14, 2016.

PARSIFAL Project-Team (section vide)

PI.R2 Project-Team

7.3. Popularization

Yann Régis-Gianas co-organised the “Journée Francilienne de Programmation”, a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS). Yann Régis-Gianas organised, and Étienne Miquey took part in the animation of the (computer science part of the) “Fête de la Science” event at the University Paris 7. Yann Régis-Gianas gave several presentations about “What is programming?” in primary and high schools of Paris and its region.

SUMO Project-Team

10.3. Popularization

Nathalie Bertrand gave an introductory talk on graph theory and its use to solve practical problems, to grad school students following the ISN (Introduction aux Sciences du Numérique) courses.

TOCCATA Project-Team

10.3. Popularization

- A. Charguéraud is one of the three organizers of the *Concours Castor informatique*http://castor-informatique.fr/. The purpose of the Concours Castor in to introduce pupils (from *CM1* to *Terminale*) to computer sciences. 475,000 teenagers played with the interactive exercises in November 2016.
- S. Boldo is a speaker for a MOOC for computer science teachers. She was also invited to Poitiers in November 2016 to discuss with teachers and present this MOOC.
- S. Boldo was invited to a panel about teaching computer science before university in Besançon in June 2016 during the GDR GPL days.
- During the "Fête de la science" on October 14th to 16th, S. Boldo gave several talks about computer arithmetic to teenagers and F. Faissole run a stand about an introduction to programming with robots.
- S. Boldo and F. Voisin did an introduction to computer science with an activity on computer hardware as a 1-hour extracurricular activity in schools for pupils in *CM1-CM2* on October 4th.
- S. Boldo gave a talk during a girls & maths weekend on November 22nd. See http://www.animath.fr/spip.php?article2897&lang=fr.

VERIDIS Project-Team (section vide)

CARTE Team

8.3. Popularization

Nazim Fatès contributed to the collective book *Lettres à Turing* (ed. Thierry Marchaisse, May 2016), which addresses the legacy of Turing in our Modern Times. He was invited to discuss this book and the question of artificial intelligence in three national radio programs:

- France Culture, La marche des sciences, “Cher alan Turing”, 1 hour, with Aurélie Luneau, 23 June 2016.
- RFI, Autour de la question, “Que devons-nous à Alan Turing?”, 1 hour, with Sophie Joubert, 24 June 2016.
- RFI, Autour de la question, “Jusqu’où ira l’intelligence artificielle?”, 1 hour, with Sophie Joubert, 7 October 2016.

Nazim Fatès participated to an open discussion (table ronde) on the theme of artificial intelligence (“Intelligence artificielle : quel monde prépare-t-elle ?”), invitation by the Cercle universitaire of Enghien-les-bains, on the 27th of Septembre in Enghien-les-bains. He was interviewed by Eric Chaverou, journalist at France Culture for his radio program of May 20, 2016, on the theme: “L’intelligence artificielle made in France”. This interview is available on the website of the radio program or directly via soundcloud. He participated to a public debate on the theme “Jusqu’où ira l’intelligence artificielle ?” the Café des sciences et techniques, organised by the CNAM, in Épinal, 21 January 2016.

COMETE Project-Team (section vide)

DICE Team

9.3. Popularization

Aurélien Faravelon: 12/05/2016, Débats Citoyens, Musée Galo Romain de Lyon

Robert Riemann: 28/12/2016, Chaos Communication Congress/We fix the Net assembly, Hambourg

PESTO Project-Team

10.3. Popularization

- Vote Électronique. Véronique Cortier. 1024 – Bulletin de la société informatique de France. Numéro 9, Novembre 2016.
- How to Explain Modern Security Concepts to your Children. Xavier Bultel, Jannik Dreier, Pascal Lafourcade, Malika More. Cryptologia, Taylor & Francis, 2016. [13]
- Comment sécuriser les communications ? Du bon usage des protocoles et de la cryptographie. Vincent Cheval, Joseph Lallemand – Séminaire *La Pépinière 4.1*, Oct 2016, Maisons pour la science au service des professeurs, Nancy.

PRIVATICS Project-Team

9.3. Popularization

9.3.1. Interview

Privatics team has participated to an episode of X:enius entitled: "Données personnelles : à quel point sommes-nous prévisibles ?". It features an interview of Claude Castelluccia, Daniel Le Métayer and Mathieu Cunche. The episode was broadcasted the 12th december 2016 on Arte.

9.3.2. Articles

D. Le Métayer in *France Stratégie, Algorithmes, libertés et responsabilités*, 10/03/2016.

C. Castelluccia in Le Monde, *Que reproche-t-on au TES, le « mégafichier » des 60 millions de Français*, 08/11/2016.

M. Cunche and C. Matte in GNU/Linux Magazine HS 84, *Traçage Wi-Fi : applications et contre-mesures*, 05/2016.

M. Cunche in Arte Futuremag, *Données personnelles, nos smartphones nous espionnent-ils?*, 05/2016.

9.3.3. Conferences

C. Castelluccia, *An Introduction to DataVeillance (Data + Surveillance)*, LIG UGA Keynote, 07/04/2016

V. Roca, *Vie privé et smartphones font ils bon ménage?*, Cours Universite´ Ouverte, Lyon 1, cycle Impact de l'informatique sur la socie´te´ et sur nos vies, 11/2016.

C. Lauradoux, *Email et vie privée: pourquoi utiliser GPG ?*, Cours Master 2, 01/12/2016

C. Lauradoux, *Cryptographie et grands nombres*, Olympiades académiques de Mathématiques, 04/07/2016

C. Lauradoux, *Cryptographie visuelle*, Collège/Lycée Jean Prévost, 01/06/2016

C. Lauradoux, *Cryptanalyse*, stage MathC2+, 06/2016

C. Lauradoux, *Protéger la confidentialité de ces messages*, Collège Paul Fort Is sur Tille, 04/10/2016

C. Lauradoux, *Internet et vie privée*, Collège Poncet Cluses, 15/12/2016

PROSECCO Project-Team

9.3. Popularization

9.3.1. Seminars

- Karthikeyan Bhargavan: invited talks at SSTIC, EUROCRYPT, OAuth Workshop
- Bruno Blanchet: invited talks at John Mitchell's 60th birthday workshop, Stanford University, CA (May 2016), Facebook, Menlo Park, CA (May 2016), and at University of Oslo (Dec 2016).
- Catalin Hritcu: invited talks at CEA List, MSR Redmond, Inria Gallium, Secure Compilation Meeting, ERC, Inria Prosecco, MPI-SWS
- Harry Halpin: invited talks at NetFutures 2016 (April 2016), Trust in the Digital World (June 2016), Strategic Research Challenges in Privacy-Enhancing Technologies (July 2016), European Dialogue on Internet Governance (September 2016), Internet Governance Forum Tunis (October 2016), Keynote at International Workshop on Semantic Web, and Cryptodesign (November 2016).

TAMIS Team

10.3. Popularization

- Vulnerability Prediction Against Fault Attacks , N. Jafri, A. Legay, J.-L. Lanet, Ercim news 106, 2016
- Skyfall : Tombé du ciel, J.-L. Lanet, Interstices, 2016 In this publication we revisit the movie Skyfall and explain on which scientific background rely some elements of the movie.
- FIC 2016 Internet des objets : la nouvelle fragilité ? We have been invited to participate at a panel with layers, IoT designer to discuss the security of the IoT.
- Atlantico, Et si les objets connectés étaient la plus grande faille qu'entreprises et particuliers pouvaient offrir aux hackers ? January 2016. In this interview we explain that the security is not the main concern of low end IoT, which is not the case with high end IoT.