Activity Report 2015

Section Popularization
Algorithmics, Computer Algebra and Cryptology

1. ARIC Project-Team ................................................................. 5
2. CARAMEL Project-Team .......................................................... 6
3. CASCADE Project-Team (section vide) ...................................... 7
4. CRYPT Team (section vide) ....................................................... 8
5. GALAAD2 Team (section vide) ................................................. 9
6. GEOMETRICA Project-Team (section vide) .............................. 10
7. GRACE Project-Team .............................................................. 11
8. LFANT Project-Team .............................................................. 12
9. POLSYS Project-Team ............................................................ 13
10. SECRET Project-Team .......................................................... 14
11. SPECFUN Project-Team ......................................................... 15
12. VEGAS Project-Team ........................................................... 16

Architecture, Languages and Compilation

13. ALF Project-Team (section vide) ............................................. 17
14. ATEAMS Project-Team ......................................................... 18
15. CAIRN Project-Team (section vide) ....................................... 19
16. CAMUS Team ................................................................. 20
17. COMPSYS Project-Team ....................................................... 21
18. CORSE Team (section vide) ................................................ 22
19. DREAMPAL Project-Team ..................................................... 23
20. POSTALE Team ................................................................. 24
21. TASC Project-Team ............................................................ 25

Embedded and Real-time Systems

22. AOSTE Project-Team (section vide) ....................................... 26
23. CONVECS Project-Team ......................................................... 27
24. HYCOMES Team .............................................................. 28
25. MUTANT Project-Team ........................................................ 29
26. PARKAS Project-Team (section vide) .................................... 30
27. POSET Team (section vide) ................................................ 31
28. SPADES Project-Team ........................................................ 32
29. TEA Project-Team (section vide) ........................................... 33

Proofs and Verification

30. ANTIQUE Project-Team (section vide) .................................. 34
31. CELTIQUE Project-Team ...................................................... 35
32. DEDUCTEAM Team .......................................................... 36
33. ESTASYS Team ............................................................... 37
34. GALLIUM Project-Team ...................................................... 38
35. MARELLE Project-Team (section vide) ................................ 39
36. MEXICO Project-Team (section vide) .................................... 40
37. PARSIFAL Project-Team ..................................................... 41
38. PLR2 Project-Team (section vide) .................................................. 42
39. SUMO Project-Team (section vide) .................................................. 43
40. TOCCATA Project-Team ................................................................. 44
41. VERIDIS Project-Team ................................................................. 45

SECURITY AND CONFIDENTIALITY
42. CARTE Project-Team ................................................................. 46
43. CASSIS Project-Team ................................................................. 47
44. COMETE Project-Team (section vide) ........................................... 48
45. DECENTRALISE Team ................................................................. 49
46. DICE Team ................................................................................. 50
47. PRIVATICS Project-Team ............................................................ 51
48. PROSECCO Project-Team ............................................................. 52
ARIC Project-Team

10.3. Popularization

Nicolas Brisebarre co-organizes scientific conferences, called «Éclats de sciences», at Maison du Livre, de l’Image et du Son in Villeurbanne. Around three conferences take place per year.

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l’Informatique. She led a "Coding morning” for Inria assistants at Montbonnot (February 2015). She gave two conferences for high-school teachers (Montbonnot, February and Grenoble, May 2015). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Simone Veil (Châtillon d’Azergues) and Mondial des Métiers (both in March 2015). She gave conferences for Rallye des Maths (May 2015) and during the Science Fair (2 high-school classes, October 2015). During the Science Fair, she was also present one afternoon at Médiathèque du Bachut - Lyon 8e. She presented computer science unplugged for primary school pupils (CM1, École Guilloux, St-Genis-Laval: 8 lectures of 45mn each) and computer science plugged (CM2, École Guilloux, St-Genis-Laval: 10 lectures of 1h in 2015-2016, 2 classes). She presented this work during Forum Maths Vivantes (October 2015). She also met people from Ébulliscience and FERS (Fondation Entreprise Réussite Scolaire) to give advice on their projects of popularization of computer science towards primary schools and high school pupils.
10.3. Popularization

- Jérémie Detrey gave a presentation on the Enigma machine and its cryptanalysis to high-school teachers as part of the journée EPI-ISN.
- Laurent Grémy has given in April an introductory course about the Diffie-Hellman protocol for high school students during a discovery day of the Université de Lorraine.
- Pierre-Jean Spaenlehauer has participated in a session “activités débranchées” organized by Marie Duflot-Kremer (MCF Univ. Lorraine) during the event MathC2+ which was held in CRI Nancy – Grand Est. The aim of this session was to provide junior high school students with an initiation to computer science through a set of algorithmic games.
- Pierre-Jean Spaenlehauer has animated a stand in the “Village des Sciences du Loria” in April 2015.
CASCADE Project-Team (section vide)
CRYPT Team (section vide)
GALAAD2 Team (section vide)
10.3. Popularization

- D. Augot gave a lecture about bits, exclusive-or, coding and digital pictures, at Lycée de la vallée de Chevreuse (Jan 22)
- D. Augot, N. Duhamel, A. Guillevic, J. Lavauzelle, D. Lucas, and B. Smith participated in the Fête la Science at École polytechnique (Oct 12)
- A. Couvreur gave a conference “Les mathématiques pour protéger l’information” for the pupils of Collège Moreau in Monthléry (91).
8.3. Popularization

Damien Robert participated in a CinémaScience event to discuss with the public after a projection of the film “Imitation Game” on Alan Turing. The theme of the intervention was “The contributions of Alan Turing from computer science to cryptography”.

9.3. Popularization

Mohab Safey El Din gave a course at the “Ecole Jeunes Chercheurs 2015” of GDR IM and wrote for it a book chapter [21].
SECRET Project-Team

9.3. Popularization

- André Chailloux published a paper in the general-audience journal *La Recherche*: Calcul quantique sans erreurs.
- Gaëtan Leurent took part to the radio program *Service Public: "Mot de passe partout"*, France Inter, April 2015 [http://www.franceinter.fr/emission-service-public-mot-de-passe-partout](http://www.franceinter.fr/emission-service-public-mot-de-passe-partout)
- Anne Canteaut gave a talk on cryptography for female students in “Première” and “Terminale” attending the *Girls can code!* week organized at EPITA, August 24-29, 2015 [https://gcc.prologin.org/](https://gcc.prologin.org/).
9.3. Popularization

- A. Bostan has published, together with Kilian Raschel, a popularization article titled *Compter les excursions sur un échiquier* in the popular science magazine *Pour la Science*, the French version of the *Scientific American*. 
8.3. Popularization

Guillaume Moroz is a member of the organizing committee of the *Olympiades académiques de mathématiques*. 
ALF Project-Team (section vide)
ATEAMS Project-Team

9.3. Popularization

- Paul Klint: “Paul Klint in RTL Nieuws over het nieuwe betalingssysteem van het pgb” (radio interview).
- Paul Klint: “De evolutie van codetaal”, media appearance, NRC Handelsblad
- Paul Klint: “Première internetfilm over Nederlands informatica erfgoed”, media appearance, Automatisering Gids.
- Jurgen Vinju: OSSMETER Pitch EU Concertation Meeting - Turning cloud research into innovative software & services, March 25th 2015, Brussels, Belgium.
CAIRN Project-Team (section vide)
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 book about modern C is in preparation.

Cédric Bastoul presented lectures and activities at the Kids University event at the University of Strasbourg in November 2015.

Cédric Bastoul prepared activities for Fête de la Science at University of Paris-Sud in October 2015.
10.3. Popularization

Compsys was involved in the proposal of the inter-disciplinary project EMI, with the maison des mathématiques et de l’informatique (MMI), and the Grame laboratory (computer music). See Section 9.1.3.

Tomofumi Yuki has given a one-day lecture at the École Jeunes Chercheurs en Programmation 2015 (http://ejcp2015.inria.fr/), entitled “Research in Compilers and How it Relates to Software Engineering”.
CORSE Team (section vide)
9.3. Popularization

Philippe Marquet is vice-president of the Société informatique de France, the French learned society in computer science.

Philippe Marquet is involved in scientific popularization and co-animate the group of people interested in science popularization within the Inria Lille - Nord Europe Research Center. He is also of member of the group for networking about computer science popularization inside Inria.

He organizes and participates to the visit of classrooms on the Inria Plateau at EuraTechnologies, promoting interactions between the scientific community and secondary school students and their teachers. He organizes and/or animates events with children and/or adults in order to initiate them to code via Scratch or to computer science via unplugged activities, and more generally promoting computer science education.

Philippe Marquet is a member of the editorial board of 1024, the bulletin of the Société informatique de France that aims at showing informatics, science and technology, in all its dimensions. 1024 targets a wide audience, from high school students to researcher, including anyone interested in computer science.
POSTALE Team

9.3. Popularization

TASC Project-Team

10.3. Popularization

- A the 2015 edition of the Fête de la Science (Nantes University):
  - A workshop around *Software for sound processing in the context of the R2D2 robot* was given by Charlotte Truchet.
  - One talk on *Travel to the land of dreams: lands, monsters and fairies* was given by Nicolas Beldiceanu.
  - Two sessions discussing and answering questions around the work of professor and researcher in computer science with young persons (18 years old) was spent by Nicolas Beldiceanu and Florian Richoux.
- Charlotte Truchet wrote an article regarding *women in computer science*.
- Interview for the Web TV FranceLive on AI and games in November 2015 by Florian Richoux.
- Interview for Nantes University regarding the collaboration of Florian Richoux with Facebook in summer 2015.
- Interview of Florian Richoux in the Thinkovery magazine (number 3, April-May-June 2015) regarding Artificial Intelligence in Games.
- Interview of Florian Richoux in Rue89 in March 2015 regarding works of Google DeepMind around the Atari game.
AOSTE Project-Team (section vide)
9.3. Popularization

H. Garavel participates to the committee in charge of organizing the Aerospace Valley series of industrial conferences on formal methods.

The fifth conference, devoted to testing, held on June 16 in Toulouse and retransmitted by video-conference in Grenoble and Saclay, attracted participants from industry and academia. W. Serwe gave a talk (with Thierry Jéron, Inria Rennes), entitled “TGV: Génération de tests de conformité à partir de modèles formels”, and a talk (with Massimo Zendri, STMicroelectronics), entitled “Génération de tests basés sur les modèles pour des systèmes sur puce avec cohérence de caches”.

The sixth conference, devoted to safety, is to be held on January 26, 2016.
HYCOMES Team

8.3. Popularization

Albert Benveniste, as a member of the French Academy of Technology, has participated to an inquiry of the French Ministry of Education on the teaching of computer science in the secondary school curriculum.
9.3. Popularization

Arshia Cont appeared as expert in BFM Business TV special live event on Music and New Technology.
PARKAS Project-Team (section vide)
POSET Team (section vide)
9.3. Popularization

Gregor Gössler was the scientific organizer of an In'Tech seminar on *Embedded systems and liability. Failures, accidents: who’s to blame*\(^0\) featuring seven invited speakers and a panel. Led by the INRIA Grenoble - Rhône-Alpes research centre, the In'Tech seminars strive to offer an opportunity for SMEs, industrial operators and researchers to come together, thus promoting technology monitoring and the exchange of information among the various participants in the development of the region’s Information Sciences and Technologies.

\(^0\)http://www.inria.fr/centre/grenoble/actualites/logiciel-embarque-et-responsabilite
TEA Project-Team (section vide)
ANTIQUE Project-Team (section vide)
8.3. Popularization

- Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, given two times in high schools close to Rennes.
- Two short tutorials. One for Isabelle/HOL [41] and one for SPAN+AVISPA [42].
DEDUCTTEAM Team

9.3. Popularization

Gilles Dowek has given various popular science talks.
Gilles Dowek writes a monthly chronicle in Pour la Science.
Gilles Dowek is a member of the Scientific board of La Main à la Pâte.
ESTASYS Team

8.3. Popularization

Together with Vannes University, the team has published three high-level description articles on systems of systems [5], [6], [7].
10.3. Popularization

Jacques-Henri Jourdan is involved in the organization of the Junior Seminar of Inria Paris-Rocquencourt.


Fabrice Le Fessant is one of the main organizers of the OCaml Meetup in Paris.

Xavier Leroy gave a popularization talk on critical software and its formal verification at the computer science colloquium of University Pierre et Marie Curie.

Since 2012, the Gallium team has published a research blog at http://gallium.inria.fr/blog/, edited by Gabriel Scherer. This blog continued its activity in 2015, with 10 posts from 8 different authors.
MARELLE Project-Team (section vide)
MEXICO Project-Team (section vide)
9.3. Popularization

K. Chaudhuri organized a half-day tutorial on Abella as a satellite event of CADE 2015 in Berlin. The slides from the talk are available as [40], and the tutorial web-site is: http://abella-prover.org/tutorial. This event was co-organized with Gopalan Nadathur, professor of Computer Science at the University of Minnesota, USA.

G. Reis participated in “Fête de la Science” as an assistant to the programming activities.
PI.R2 Project-Team (section vide)
SUMO Project-Team (section vide)
TOCCATA Project-Team

10.3. Popularization

- A. Charguéraud and S. Boldo contributed to the preparation of the exercises of the Concours Castor informatique http://castor-informatique.fr/. A. Charguéraud is also one of the three organizers of this contest. The purpose of the Concours Castor is to introduce pupils (from CM1 to Terminale) to computer sciences. More than 345,000 teenagers played with the interactive exercises in November 2015.

- C. Marché, together with J. Kanig from AdaCore company, wrote an article in the ERCIM news journal [17] to advertise on the work done in the ProofInUse joint laboratory for the popularization of formal methods in the development of safety-critical Ada programs.

- S. Boldo, with T. Vieville (Mnemosyne team, Inria Bordeaux - Sud-Ouest), F. Masseglia (Zenith team, Inria Sophia Antipolis - Méditerranée and P. Bernhard (INRA) wrote a text about the TIPE 2016 (personal work before the competitive entrance in engineering schools). The topic was “Structures: organization, complexity, dynamic”. This was published on the popularization website http://pixees.fr [31].

- S. Boldo co-organized popularization talks for the administrative staff of Inria Saclay - Île-de-France. She gave a talk on January 29th about a scientific article [21] and led a coding session (with Scratch) on February 12th with A. Imperiale (M3DISIM team).

- S. Boldo co-organized the coming of teenagers from the collège Flemming in Orsay to the laboratory on May 28th and gave talks to several groups all day long.

- S. Boldo co-organized the Inria Saclay - Île-de-France Fête de la science. She created two stands (about programming) and run one on October 9th.

- S. Boldo gave a talk to the winners of the Mathematics Olympiads on June 10th in Rocquencourt.

- S. Boldo gave a talk at the “Girls can code” week on August 27th, in Paris.

- S. Boldo gave a talk to high school teenagers in Angers on October 12th.

- S. Boldo gave a talk to “Classes Préparatoires” at l’Essouriau, Les Ulis on September 24th.

- S. Boldo gave a talk at “Futur en Seine” a popularization festival in Paris and Paris area, in Orsay, on June 18th.

- C. Paulin together with I. Glas from labex DigiCosme is proposing an introduction to computer science (various activities on programming, data representation, algorithms during 6 sessions of 1 hour) as an extracurricular activity in schools for pupils in CM1-CM2.

- C. Paulin organised in 2015 the third edition of the Concours ISN of the Labex DigiCosme, supported by the Rectorat de l’Académie de Versailles. Selected projects developed by the high school pupils (Terminale) as part of their curricula in Computer Science are submitted to this contest. The best projects are selected and presented during a general event.

- C. Paulin, I. Glas, and A. Paskevich run a stand (introduction to information technologies and programming) during the “Fête de la science” Île-de-France on October 9 and 10.
VERIDIS Project-Team

10.3. Popularization

Marie Duflot-Kremer took part in various popularization activities, with a public ranging from primary school kids to high school and potential University students. A selection of these activities is given below:

- two days at “Fête de la science” in Nancy;
- a course on databases for high school professors in charge of teaching optional course ISN (Informatique et Sciences du Numérique);
- her explanations of unplugged activities have been recorded by Inria, and a Youtube channel has been created by the Interstice team to promote and share such activities;
- she is a member of two groups dedicated to the training of math teachers who will teach computer science to students of age 11 to 18;
- “Journée femmes de Sciences”: one day dedicated to the promotion of science among 14 years old girls;
- she is a member of the steering committee preparing an itinerant exposition intended for explaining computer science to the public, to be released in 2016;
- she presented a poster at the Scratch2015 conference about teaching computer programming to kids from the age of 8 years onward.

Pascal Fontaine and Stephan Merz illustrated techniques that underly formal verification of protocols and algorithms at events like “Fête de la Science”. Using wooden puzzles and Sudoku sheets, they explained how real-life problems can be represented in logical form and then solved using automated tools based on formal logic.

Martin Quinson organized a 2-days workshop for secondary math teachers on how algorithms could be used to reinforce the abilities of pupils to verbalize, set out arguments and conduct rigorous demonstrations (Nancy, March 2-3 2015). This workshop was co-organized by the IREM (Institut de Recherche en Enseignement des Mathématiques) of Nancy. He also co-organized a one day workshop for about 100 secondary computer science teachers. This event spreads the best practices to teach our topic (Nancy, March 12th 2015). Martin Quinson was a scientific expert in an experiment in which we explored how Scratch can be used to teach Computer Science in after school activities every week for the whole week. The results of this experiment, conducted in a collaboration between Inria and the MJC Nomade (Nancy) were published in [35].

Christoph Weidenbach lectured within the series “Perspektiven der Informatik” at Saarland University and within the public lecture series of the federal state of Saarland.
9.3. Popularization

- Isabelle Gnaedig is member of the scientific vulgarization committee of Inria Nancy - Grand Est. This committee is a choice and guidance instance helping the direction of the center and the person in charge of popularization events to elaborate a strategy, to realize events and to help researchers to get involved in various actions aiming at popularizing our research themes, and more generally computer science and mathematics.

- Mathieu Hoyrup wrote an article on his recent work for Images des Mathématiques.
10.3. Popularization


- Blog entries for Blog Binaire (Le Monde): Attaque à l’italienne (Véronique Cortier), Les bonnes propriétés d’un système de vote électronique (Véronique Cortier and Steve Kremer), Le vote papier est-il réellement plus sûr que l’électronique ? (Véronique Cortier), Qu’est-ce qu’un bon système de vote ? (Véronique Cortier).

COMETE Project-Team (section vide)
8.3. Popularization

- ACTUX Meeting, on “Résistance des GNUs”
- Security in Times of Surveillance (TU Eindhoven), on “Knocking down the HACIENDA with TCP Stealth”
- Linux User Group (LUG) Camp, on “Résistance des GNUs”
- Studentenforum im Tönissteiner Kreis e.V., on “State Surveillance: Benefits and Risks”
- Invest in Cyber Convention, on “La protection de la vie privée et sécurité des objets connectés” (Panel)
- Post Snowden Cryptography, on “The GNUnet: 45 Subsystems in 45 Minutes”
- Organizing YBTI workshop at 32c3 in Hamburg (December 29th)
9.3. Popularization

- Stéphane Grumbach, Comment le numérique change-t-il la société ? Cycle de conférences Homo numericus, Fête de la science, Bourg-en-Bresse, 10 octobre 2015
- Stéphane Grumbach, A qui profitent les Big Data? Soirée-débat Et si on en parlait, "La Révolution Big Data : chance ou menace?" Grand Amphithéâtre, Université de Lyon, 28 avril 2015
9.3. Popularization

Article of C.Castelluccia and D.Le Métayer in le Monde, Oui, la loi sur le renseignement prépare bien une surveillance de masse, 09/06/2015.

Article of C.Castelluccia and D.Le Métayer in Pour La Science, Renseignement : le traitement massif de données est aussi dangereux qu’inefficace, 11/06/2015.

Interview of C.Castelluccia and D.Le Métayer in le Monde, Des dizaines de milliers de personnes vont être suspectées à tort, 06/05/2015.

Article of C.Castelluccia and D.Le Métayer in La Recherche, Les failles de la loi sur le renseignement, 11/2015.

Interview of V. Roca on France Culture in Les Nouvelles Vagues, Privacy leaks in smartphones, 10/2015


Representation of Privatics by V. Roca at Journée numérique au Sénat, 11/02/2015.

Representation of Privatics by M. Cunche at Journée numérique au Sénat, 11/02/2015.


Seminar CCA of C. Lauradoux, Exploitations concrètes des mauvaises utilisations des fonctions de hashage, 12/06/2015.

Workshop of C. Lauradoux at GREHACK 2015, Sécurité des drones.

Seminar of Marine Miner at LIMOS seminar, CUBE Cipher: Une Famille de Chiffrement par Blocs Quasi-Involutifs et Facile à Masquer, 01/10/2015.

Seminar of Marine Miner at XLIM seminar, CUBE Cipher: Une Famille de Chiffrement par Blocs Quasi-Involutifs et Facile à Masquer, 10/02/2015.

Seminar of Marine Miner at Rennes, Some solutions for security of WSNs, 11/2015.
10.3. Popularization

10.3.1. Popular Press and Vulnerability Reports

The FREAK and Logjam attacks discovered by the miTLS team resulted in articles in many newspapers, magazine, and popular websites, including the New York Times, Wall Street Journal, Economist, and Wired. As a result of our discovery of these attacks and their popularization, major changes were made in all web browsers, web servers, and in the TLS protocol itself.

10.3.2. Seminars
