RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2013

Section Dissemination

Edition: 2014-03-20

ARIC Project-Team

9. Dissemination

9.1. Scientific Animation

- Florent de Dinechin is an associate editor of the journal *IEEE Transactions on Computers*. He was a member of the Program Committees of the conferences CompAs (Grenoble, January 2013), Applied Reconfigurable Computing (Los Angeles, March 2013), Highly Efficient Accelerators and Reconfigurable Technologies (Edimburgh, June 2013), Field-Programmable Logic (Porto, September 2013), Field-Programmable Technology (Kyoto, December 2013), ReConfig 2013 (Cancun, December 2013). He also organized a tutorial half-day on arithmetic core generation using the FloPoCo framework at HiPEAC 2013 (Berlin, January 2013).
- Guillaume Hanrot has been deputy director of the LIP (laboratoire d'informatique du parallélisme) since 01/01/13. He has also been in charge of the computer science master at ENS de Lyon for the academic year 2012-2013. He has been a member of hiring committees for an assistant professor position at Caen IUT, for an assistant professor position at Saint-Étienne IUT, for a professor position at ENSIIE Strasbourg, and of the national committee for "Prime d'excellence scientifique". He is a member of the scientific council of ENSIIE (Évry). He chairs a working group in charge of making recommendations concerning general teaching and training policy at ENS de Lyon.
- Claude-Pierre Jeannerod is a member of the scientific committee of "Journées Nationales de Calcul Formel".
- Fabien Laguillaumie has been member of an hiring committee for an assistant professor position at Université Lyon 1. He was member of ProvSec 2013 program committee. He is responsible for the second year "Ingénierie des Risques" of the Master SAFIR.
- Vincent Lefèvre and Nicolas Louvet were in the scientific committee of the CNRS thematic school *Précision et reproductibilité en calcul numérique* (Fréjus, France, March, 2013).
- Jean-Michel Muller co-chairs the Groupement de Recherche (GDR) *Informatique Mathématique* of CNRS. He is an associate editor of the journal *IEEE Transactions on Computers*. He participated to the evaluation committee of the LIRMM laboratory (Montpellier) in November 2013. He is a member of the scientific councils of CERFACS (Toulouse) and ENS de Lyon. He was a member of the Program Committees of the conferences IEEE ARITH 21 (Austin, Texas, April 2013) and IEEE ASAP'2013 (Washington DC, June 2013).
- Nathalie Revol was in the hiring committee for junior researchers (CR) of Inria Grenoble - Rhône-Alpes. She is a member of the CES (Commission des Emplois Scientifiques), the hiring committee for postdocs at Inria Grenoble - Rhône-Alpes. She was the chair of the organization committee and took charge of the "gender aspects" of the Forum 2013 des Jeunes Mathématicien-ne-s, 13-15 November, Lyon. She is a member of the "comité de diffusion" of the MILyon labex. She belongs to the steering committee for the MMI (Maison des Mathématiques et de l'Informatique). She is a member of the selecting committee of CapMaths.
- Bruno Salvy is a member of the editorial boards of the "Journal of Symbolic Computation", of the "Journal of Algebra" (section Computational Algebra) and of the collections "Texts and Monographs in Symbolic Computation" (Springer) and "Mathématiques et Applications" (SMAI-Springer). He is organizing the working group Computer Algebra of the CNRS GDR IM. This year, he has been in the program committees of ISSAC 2013 (Boston, Mass., June 2013) and Analco 2013 (New Orleans, Louisiana, January 2013).

- Damien Stehlé has been deputy director and Erasmus coordinator of the ENS de Lyon Computer Science department from 01/01/13 until 30/06/13. He has been the director of the Computer Science department since 01/07/13. He is a member of the steering committee of the Cryptography and Coding CNRS working group (GdT C2 du GDR IM). He is a member of the steering committee of the PQCrypto conference series. In 2013, he served in the program committees of the PQCrypto (Limoges, France, June 2013) and Asiacrypt (Bengalore, India, December 2013) conferences.
- Gilles Villard is chair of LIP laboratory and a member of the editorial board of the "Journal of Symbolic Computation."

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Nicolas Louvet, *Computer Architecture*, 74h, L2, Univ. Lyon 1.

Licence : Nicolas Louvet, *Algorithms and Data Structures*, 30h, L3, Univ. Lyon 1.

Licence : Nicolas Louvet, *Operating Systems*, 50h, L3, Univ. Lyon 1.

Master: Nicolas Brisebarre and Bruno Salvy, *Approximations: from symbolic to numerical computation, and applications*, 24h, ENS de Lyon.

Master: Guillaume Hanrot and Jean-Michel Muller, *Computer Algebra*, 24h, ENS de Lyon.

Master: Claude-Pierre Jeannerod, Nicolas Louvet, Nathalie Revol, *Numerical Algorithms*, 48h, Univ. Lyon 1.

Master: Fabien Laguillaumie, *Cryptography, Error Correcting Codes*, 150h, Univ. Lyon 1.

Master: Vincent Lefèvre, *Computer Arithmetic*, 14h, Univ. Lyon 1.

Master: Jean-Michel Muller, *Floating-Point Arithmetic and Formal Proof* (8h + coordination of the 24h course), ENS de Lyon.

Master: Bruno Salvy, *Computer Algebra*, 12h, MPRI.

Master: Damien Stehlé, *Cryptography*, 24h, ENS de Lyon.

Doctorat: Nicolas Brisebarre, *Lattices in computer arithmetic*, 3h, École de Printemps d'Informatique Théorique, Autrans, March 21.

Doctorat: Florent de Dinechin, *Arithmétique flottante*, 1h30, École CNRS *Précision et reproductibilité en calcul numérique*, Fréjus, March 25-29.

Doctorat: Guillaume Hanrot, *Introduction to lattice algorithms*, 3h, École de Printemps d'Informatique Théorique, Autrans, March 18.

Doctorat: Vincent Lefèvre, *Arithmétique flottante en précision arbitraire*, 3h, École CNRS *Précision et reproductibilité en calcul numérique*, Fréjus, March 25-29.

Doctorat: Jean-Michel Muller, *Arithmétique flottante*, 2h, École CNRS *Précision et reproductibilité en calcul numérique*, Fréjus, March 25-29.

Doctorat: Jean-Michel Muller, *Arithmétique flottante*, 2h, École HPC, Lyon, September 3.

Doctorat: Nathalie Revol and Philippe Théveny, *Arithmétique flottante et intervalles*, 3h, École CNRS *Précision et reproductibilité en calcul numérique*, Fréjus, March 25-29.

Doctorat: Nathalie Revol and Philippe Théveny, *Précision et arithmétique flottante : outils, bibliothèques*, 3h30, JDEV : Journées du Développement Logiciel, École Polytechnique, 4-6 September.

Doctorat: Nathalie Revol and Philippe Théveny, *Introduction à l'arithmétique par intervalles*, 3h, professional training entitled "Contrôler et améliorer la qualité numérique d'un code de calcul industriel", Collège de l'X, Paris, 21-22 November.

Doctorat: Damien Stehlé, *Introduction to lattices*, 3h, École de Printemps d'Informatique Théorique, Autrans, March 18.

9.2.2. Supervision

PhD: Julien Devigne, *Protocoles de re-chiffrement pour le stockage de données*, September 2011 - December 2013 (Orange Labs - Univ. Caen); co-supervised by Fabien Laguillaumie (together with Sébastien Canard and Brigitte Vallée).

PhD in progress: Nicolas Brunie, *Architecture et réalisation d'un accélérateur reconfigurable à couplage fort pour processeurs parallèles*, since September 2010 (CIFRE Kalray from April 2011); co-supervised by Florent de Dinechin (and Renaud Ayrignac).

PhD in progress: Louis Dumont, *Algorithmique efficace pour les diagonales*, since September 2013, co-supervised by Bruno Salvy (together with Alin Bostan).

PhD in progress: Silviu Filip, *Filtroptim : tools for an optimal synthesis of numerical filters*, since September 2013, co-supervised by Nicolas Brisebarre and Guillaume Hanrot.

PhD in progress: Pierre Lairez, *Algorithmique efficace pour la création télescopique et ses applications*, since September 2011, co-supervised by Bruno Salvy (together with Alin Bostan).

PhD in progress: Adeline Langlois, *Foundations of lattice-based cryptography*, since September 2010, supervised by Damien Stehlé.

PhD in progress: Vincent Neiger, *Multivariate interpolation in computer algebra: efficient algorithms ans applications*, since September 2013, co-supervised by Claude-Pierre Jeannerod and Gilles Villard (together with Éric Schost).

PhD in progress: Marie Paindavoine, *Méthodes de calculs sur des données chiffrées*, since October 2013 (Orange Labs - UCBL), co-supervised by Fabien Laguillaumie (together with Sébastien Canard).

PhD in progress: Philippe Théveny, *Numerical quality and high performance in scientific computing on emerging architectures*, since September 2011, supervised by Nathalie Revol.

PhD in progress: Serge Torres, *Some tools for the design of efficient and reliable function evaluation libraries*, since September 2010, co-supervised by Nicolas Brisebarre and Jean-Michel Muller.

9.2.3. Juries

- Nicolas Brisebarre was a member of the PhD committee of Răzvan Bărbulescu (Nancy, December 2013).
- Guillaume Hanrot was an external referee for the PhD of Md Mohammed Haque (Macquarie U., Australia, sept. 2013) and for the PhD of Mariya Georgieva (Caen, 2013-12-09). He was a member of the committee for the PhD of Léo Ducas (ENS Paris, 2013-11-12) and Yuanmi Chen (ENS Paris, 2013-11-13).
- Fabien Laguillaumie was an external referee for the PhD of Léo Ducas (ENS Paris, 2013-11-12) and Viet Cuong Trinh (Univ. Paris 8, 2013-12-19). He was a member of the PhD committees of Mario Stefler (2013-09-26, ENS Paris), Nicolas Estibals (2013-10-30), Mariya Georgieva (Caen, 2013-12-09), and Aurore Guillevic (ENS Paris, 2013-12-20)
- Jean-Michel Muller was a referee for the habilitation of Stef Graillat (U. Paris 6, 2013-12-2).
- Nathalie Revol was the external referee for the PhD of Bingzhou Zheng (U. McMaster, Hamilton, Canada, 2013-12-10).
- Bruno Salvy was a member of the PhD committee of Fabien Monfreda (Toulouse, July 2013).
- Damien Stehlé was an external referee for the PhD of Romar Basillaje Dela Cruz (Nanyang Technological U., Singapore, March 2013) and of Zhenfei Zhang (U. of Wollongong, Australia, October 2013).

9.3. Invited Conferences

- Florent de Dinechin gave invited talks or lectures at the CERN/Intel OpenLab workshop at CERN, at the LIF seminar in Luminy, at the Intel Summer School in Nizhniy Novgorod, and at the Journées Développement Logiciel (JDEV) in Palaiseau.
- Jean-Michel Muller gave an invited talk *Proof of Properties in Floating-Point Arithmetic* at the conference *Continuity, Computability, Constructivity - From Logic to Algorithms* (CCC 2013), Swansea University/Gregynog, UK, June 26–30, 2013.
- Nathalie Revol gave talks about numerical reproducibility, with a focus on interval computations, at PPAM'2013 (Warsaw, Poland, 2013/09/8-11), at RAIM 2013 (Paris, France, 2013/11/18-20), at McMaster University (Hamilton, Ontario, Canada, 2013-12-10), and at University of Toronto (Ontario, Canada, 2013-12-13).
- Bruno Salvy was invited to give a talk *Implicit Species at the basis of Analytic Combinatorics* at the 24th International Meeting on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithm (AofA 2013, Menorca, Spain, May 27–31) and on *Newton iteration in computer algebra and combinatorics* at the *Journées d'Informatique Fondamentale de Paris Diderot* (April 22–26).
- Damien Stehlé gave an invited lecture talk at *Journées Nationales du Calcul Formel* (Luminy, France, May 13–17, 2013), invited plenary talks at the conferences *SIAM Conference on Applied Algebraic Geometry (AG13)* (Fort Collins, Colorado, USA, August 1–4, 2013) and *ICISC* (Seoul, Korea, November 25–29, 2013) and at the *Microsoft Research India Workshop on Lattice-Based Cryptography* (Bengalore, India, November 30, 2013).

9.4. Popularization

- Nathalie Revol gave talks for pupils at collèges and lycées, as an incentive to choose scientific careers: lycée Jeanne d'Arc (Cessy, Ain), lycée Rosa Parks (Neuville, Rhône). During the "Week of mathematics", she gave a 2-hour talk at lycée de la Plaine de l'Ain (Ambérieu-en-Bugey, Ain). She was present, took part in speed-meetings, and gave talks for the "Mondial des Métiers" (Eurexpo Lyon, Chassieu, Rhône) and for "Science au Carré(e)" (Forum des Halles, Paris). For the Science Fair, she gave 8 talks at ENS de Lyon. She was invited to "Interacadémiques" in Lyon, for an audience of inspecteurs d'académie. She supervised the internship of Quentin Chopinet (1e S, one week) and hosted Elsa Courtais (spé TSI, one day).
- Damien Stehlé was interviewed for an article in *La Recherche*, published in September 2013.

CARAMEL Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Caramel seminar

Sixteen speakers were invited to our seminar in 2013: Pierre-Jean Spaenlehauer, Maike Massierer, Emmanuel Jeandel, Jérémy Parriaux, Adeline Langlois, Antoine Joux, François Morain, Mourad Gouicem, Hamza Jeljeli, Svyatoslav Covanov, Alice Pellet-Mary, Bastien Vialla, Julia Pieltant, Clément Pernet, Cécile Pierrot, and Luca De Feo.

9.1.2. Joint security seminar with the university master in informatics

The team is involved with other teams and the university master in informatics in the organization of the security seminar which started in 2013. Six speakers were invited during the last months of 2013: Olivier Heen, Frédéric Raynal, Stéphanie Lacour, Alexandre Dulaunoy, Vincent Strubel and Cédric Blancher.

9.1.3. Committees memberships

- Jérémie Detrey
  - was a member of the program committee of the International Conference on Pairing-Based Cryptography (Pairing 2013).
- Pierrick Gaudry
  - was a member of the program committee of the ASIACRYPT 2013 conference,
  - was in a hiring committee (Comité de Sélection) in Université de Lorraine.
- Emmanuel Thomé
  - is an elected member of the Inria Evaluation Committee for the period 2011-2014,
  - is an elected member of the Inria Nancy *Comité Hygiène, Sécurité, et Conditions de Travail*,
  - is an appointed member of the Inria Nancy *Comité de développement durable*,
  - is a member of the *Bureau du département de formation doctorale* in computer science at Université de Lorraine,
  - was in a hiring committee (Comités de Sélection) in Université de Lorraine,
  - was in the hiring committee for the Inria *Chargé de recherches* positions both in Bordeaux and Rocquencourt.
- Marion Videau
  - is a member of the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
  - is a member of the program committee of the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2013),
  - was a member of the program committee of the 16th annual International Conference on Information Security and Cryptology (ICISC 2013),
  - is an elected member of the LORIA laboratory council,
  - is a member of the *Commission des développements technologiques* (CDT) of the Inria-NGE research center.
- Paul Zimmermann

- is an elected member of the Inria Scientific Board,
- is (from September) "délégué scientifique´´ of the Nancy Grand Est center, and as a consequence member of the Inria Evaluation Committee.

9.1.4. Invited Conferences

- Pierrick Gaudry was invited to give a talk at the Workshop on Elliptic Curve Cryptography (ECC 2013) in Leuven, Belgium and to give two lectures at the Summer School that preceded it; he was invited to give a talk at the Pairing 2013 conference in Beijing, China; he was also invited to give a talk at the Workshop on Emerging Applications of Finite Fields at Linz, Austria.

9.1.5. Calcul mathématique avec Sage

Together with nine other colleagues, Paul Zimmermann wrote a book about doing mathematics with Sage [18]. This book is available in electronic version under a Creative Commons license, and is also available in paper form from Amazon under a very low price.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Jérémie Detrey:
  - Security of websites: 2 hours (lecture), L1, IUT Charlemagne, Nancy, France.
- Pierrick Gaudry
  - Algorithmic Number Theory: 5 hours (lectures), M2, University Paris 7 (Master Parisien de Recherche en Informatique), Paris, France.
- Emmanuel Thomé:
  - Cryptology: 24 hours, M1, ESIAL, Nancy, France.
  - Introduction to cryptology: 3 hours (lecture), M2, École des Mines de Nancy, France.
  - Training for "Informatique et Sciences du Numérique", Cryptology, Networks: 9 h, Université de Lorraine, Nancy, France. (Training for high school teachers who intend to teach this topic in high school).
- Marion Videau, teaching at the faculty of technology and sciences, Université de Lorraine, Nancy, France:
  - Introduction to algorithmic and programming: 40 hours (lectures and tutorial sessions), 20 hours (practical sessions), L1.
  - Programming methodology in C: 21 hours (lectures and tutorial sessions), L1.
  - Students supervisor for about 12 L1 students: 12 hours, L1.
  - Introduction to information system security: 15 hours (lectures), 15 hours (tutorial sessions), M1.
  - Information System Security: 21 hours (lectures and tutorial sessions), M2, IGA, Maroc
  - Information System Security: 12 hours (lectures and tutorial sessions), M2
  - Software Validation, Verification and Certification: 12 hours (lectures and tutorial sessions), M2
  - Supervision of two M1 students for their *Introduction to research* practical course throughout one semester
  - Supervision of M2 students projects: 15 hours
  - Supervision and jury of M2 students internships: 10 hours.
  - Responsability of the M2 *parcoursServices, Sécurité des Systèmes et des Réseaux / Sécurité des Architectures Web*

9.2.2. Internships

- Svyatoslav Covanov, École Polytechnique, "Fürer's integer multiplication algorithm", Apr–July 2013, supervised by Emmanuel Thomé.
- David Lucas, Télécom Nancy, "Recherche de bitcoins : implémentation et accélération sur le MPPA-256 de Kalray", May–Jul 2013, supervised by Jérémie Detrey.
- Fabien Nollet, Télécom Nancy, "Parallelization of the multiplication of polynomials over $\mathrm{GF}(2)$", May–Jul 2013, supervised by Emmanuel Thomé.
- Alice Pellet Mary, ÉNS Lyon, "Test rapide de cubicité modulaire", Jun–Jul 2013, supervised by Pierrick Gaudry.
- Alexandre Talon, ÉNS Lyon, "Non linear polynomial selection for NFS´´, Jun–Jul 2013, supervised by Paul Zimmermann.
- Sébastien Vandeneeckhoutte, Télécom Nancy, "Énumération efficace des polynômes irréductibles sur un corps fini" Feb–Jun, 2013, supervised by Marion Videau and Pierrick Gaudry.

9.2.3. Supervision

Defended PhDs:

- Nicolas Estibals, "Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques", started in 2009, co-supervised by Jérémie Detrey and Pierrick Gaudry [9]. Defended on 2013/10/30.
- Răzvan Bărbulescu, "Number and function field sieve for discrete logarithm", started in 2011, supervised by Pierrick Gaudry [8]. Defended on 2013/12/04.

PhD in progress:

- Hamza Jeljeli, "Using graphics accelerators for problems arising in the Number Field Sieve and Function Field Sieve algorithms", started in 2011, supervised by Jérémie Detrey and Emmanuel Thomé.
- Cyril Bouvier, "Integer Factoring on High-Performance Architectures", started in 2012, supervised by Paul Zimmermann.
- Laurent Grémy, "Analysis and optimization of sieves arithmetic algorithms" started in oct. 2013, co-supervised by Pierrick Gaudry and Marion Videau.
- Hugo Labrande, "Explicit computation of isogenies between Jacobians of curves using a complex analytic method", started in sep. 2013, cotutelle supervision between Emmanuel Thomé and Michael J. Jacobson, University of Calgary.

9.2.4. Juries

- Jérémie Detrey
  - was a member of the jury of the Polytechnique/ÉNS competitive entrance exam,
  - was a member of the PhD thesis jury of Nicolas Estibals (Université de Lorraine).
- Pierrick Gaudry was a member of the PhD thesis jury of Razvan Barbulescu (Université de Lorraine), Nicolas Estibals (Université de Lorraine), Jean-Gabriel Kammerer (Université de Rennes 1), Aurore Guillevic (École Normale Supérieure), Louise Huot (Université de Paris 6).
- Emmanuel Thomé was a member of the PhD thesis jury of Kisoon Yoon (Université de Caen Basse-Normandie).
- Marion Videau was president of one of the scientific baccalaureate juries in Nancy in July 2013.

9.3. Popularization

- Jérémie Detrey gave a presentation on the Enigma machine and its cryptanalysis to high-school teachers as part as the "journée EPI-ISN".

- Pierrick Gaudry gave a presentation at the "journée de l'Association francophone des spécialistes de l'investigation numérique".
- Marion Videau:
  - gave a talk for the awards ceremony of the *Olympiades de maths* in Lorraine.
  - gave a practical session of cryptography and information security for students from *lycées* taking part in an immersion day at the faculty.
  - participated to events on information about university studies for pupils and students (Clés de la réussite, Portes ouvertes de la faculté des sciences, Oriaction).
- Paul Zimmermann takes part in the "Maths-en-Jeans" program, with about 20 students in "troisième" at the Collège Pierre Brossolette in Réhon.

CASCADE Project-Team

6. Dissemination

6.1. Editorial Boards

Editor-in-Chief

- of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: David Pointcheval

Associate Editor

- of *Security and Communication Networks*: David Naccache (editor)
- of *Journal of Cryptographic Design*: David Naccache (editor)
- of *Encyclopedia of Cryptography and Security*: David Naccache (editor)
- of *Journal of Computer Security, IOS Press*: David Naccache (associate editor)
- of *Open Journal of Information Security and Applications, SOP*: David Naccache (editor)
- of *Cryptologia* – Taylor & Francis: David Naccache (editor)
- of *Information Processing Letters* – Elsevier: David Pointcheval
- of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla
- of *IET Information Security*: Michel Abdalla

Columnist (in charge of the bi-monthly CryptoCorner)

- of the *IEEE Security and Privacy Magazine*: David Naccache

6.2. Program Committees

- FIC - January, Lille, France: David Naccache
- ComManTel - January, Ho Chi Minh City, Vietnam: David Naccache
- PKC - February, Nara, Japan: David Naccache
- CT-RSA - February, San Francisco, USA: Michel Abdalla
- IIT - March, Al Ain, UAE: David Naccache
- WAHC - April, Okinawa, Japan: David Naccache
- LightSec - May, Gebze, Turkey: David Pointcheval
- Eurocrypt - May, Athens, Greece: Vadim Lyubashevsky
- ASIACCS - May, Hangzhou, China: David Naccache
- HOST - June, Austin, Texas, US: David Naccache
- ACISP - July, Brisbane, Australia: Michel Abdalla
- SECRYPT - July, Reykjavik, Iceland: David Naccache
- Indocrypt - July, Mumbai, India: David Naccache
- Crypto - August, Santa Barbara, USA: Vadim Lyubashevsky
- ICACCI (SSCC) - August, Mysore, India: David Naccache
- CHES - August, Santa Barbara, CA, USA: David Naccache
- SPACE - October, Kharagpur, India: David Naccache
- IWSEC - November, Okinawa, Japan: Damien Vergnaud
- RIVF - November, Hanoi, Vietam: David Naccache

- ICICS - November, Beijing, China: David Pointcheval, David Naccache
- Pairing - November, Beijing, China: Damien Vergnaud
- ISC - November, Dallas, Texas: David Naccache
- SBSeg - November, Manaus, Brazil: Michel Abdalla (Program Chair)
- ACM CCS - November, Berlin, Germany: David Naccache
- CANS - November, Paraty, Brazil: Michel Abdalla (Program Chair), Damien Vergnaud
- CARDIS - November, Berlin, Germany: David Naccache
- Asiacrypt - December, Bengaluru, India: Michel Abdalla, David Pointcheval, Hoeteck Wee
- IMACC - December, Oxford, UK: David Naccache
- Botconf - December, Nantes, France: David Naccache

6.3. Teaching - Supervision - Juries

6.3.1. Teaching

- Licence: David Naccache, Introduction to computer science, L1, Univ. Paris II
- Master: David Naccache, Scientific programming through practice, M1, ENS
- Master: David Naccache, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS
- Master: Michel Abdalla, David Pointcheval, Vadim Lyubashevsky, Cryptography, M2, MPRI
- Master: David Naccache, Computer Security, M2, Univ. Paris II
- Master: David Naccache, Computer Security, M2, Beijing Jiaotong University
- Master: David Naccache, Risk Management, M2, Univ. Paris II
- Master: David Naccache, Computer Forensics, M2, Univ. Paris II
- Master: David Naccache, Computer Security, M2, University of Luxembourg
- Master: David Pointcheval, Cryptography, M2, ESIEA

6.3.2. Supervision

- PhD: Jérémy Jean, Cryptanalyse de primitives symétriques basées sur le chiffrement AES, September 24th 2013, Pierre-Alain Fouque
- PhD: Mario Strefler, Diffusion chiffrée avec traçage de traîtres, ENS, September 26th 2013, David Pointcheval
- PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen
- PhD: Patrick Derbez, Attaques par rencontre par le milieu sur l'AES, ENS, December 9th 2013, Pierre-Alain Fouque
- PhD: Aurore Guillevic, Étude de l'arithmétique des couplages sur des courbes algébriques pour la cryptographie, ENS, December 20th 2013, Phong Nguyen & Damien Vergnaud
- PhD in progress: Tancrède Lepoint, Lattice-based cryptography, 2011, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Sylvain Ruhault, Randomness in cryptography, 2011, David Pointcheval & Damien Vergnaud
- PhD in progress: Sonia Belaid, Leakage-resilient cryptography, 2012, Michel Abdalla
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, 2012, Michel Abdalla & David Pointcheval
- PhD in progress: Diana Maimut, Fully Homomorphic Encryption, 2012, David Naccache

- PhD in progress: Thomas Prest, Lattice-based cryptography, 2012, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Olivier Sanders, Delegation of computations, 2012, David Pointcheval
- PhD in progress: Mario Cornejo, Security for the cloud, 2013, Michel Abdalla
- PhD in progress: Alain Passelègue, Security against related-key attacks , 2013, Michel Abdalla
- PhD in progress: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, 2013, Damien Vergnaud
- PhD in progress: Houda Ferradi, Biometric protocols and mobile security, 2013, David Naccache
- PhD in progress: Simon Cogliani, Authenticated Encryption, 2013, David Naccache

6.3.3. Juries

- PhD: Maria Christofi *Preuves de sécurité outillées d'implémentations cryptographiques* Univ. Versailles – Saint-Quentin, February 15th 2013: David Naccache
- PhD: Alfredo Rial, *Privacy-Preserving E-Commerce Protocols*, KU Leuven, Belgium, March 28th 2013: David Pointcheval
- HDR: Jessy Clédière *Treize années au Centre d'Evaluation de la Sécurité des Technologies de l'Information du CEA-Grenoble (CESTI-Léti)* Institut Néel (CNRS), Grenoble, June 19th 2013: David Naccache
- PhD: Alex Ruiz, *Contributions to Secret Sharing and Other Distributed Cryptosystems*, Univ. Politècnica de Catalunya, July 22nd 2013: Michel Abdalla
- PhD: David Oswald *Implementation Attacks: From Theory to Practice* Univ. Bochum, Germany, August 1st 2013: David Naccache
- HDR: Valérie Nachef *Cryptographie, Attaques génériques, Authentification* Univ. Cergy-Pontoise, September 25th 2013: David Naccache
- PhD: Mario Strefler, *Diffusion chiffrée avec traçage de traîtres*, ENS, September 26th 2013: David Pointcheval (supervisor), David Naccache
- PhD: Léo Ducas, *Signatures Fondées sur les Réseaux Euclidiens: Attaques, Analyses et Optimisations*, Univ. Paris 7, November 12th 2013: David Pointcheval, Vadim Lyubashevsky
- PhD: Jannik Dreier, *Formal Verification of Voting and Auction Protocols: From Privacy to Fairness and Verifiability*, Univ. Grenoble, November 25th 2013: David Pointcheval (chair)
- PhD: Sébastien Tiran *Side Channels in the Frequency Domain* Univ. Montpellier 2, December 11th 2013: David Naccache
- PhD: Patrick Derbez, *Attaques par Rencontre par le Milieu sur l'AES*, ENS, December 9th 2013: David Pointcheval
- PhD: Julien Devigne, *Protocoles de re-chiffrement pour le stockage de données*, Univ. de Caen – Basse-Normandie, December 13th 2013: Damien Vergnaud
- PhD: Viet Cuong Trinh, *Sécurité et efficacité des schémas de diffusion de données chiffrés*, Univ. Paris 8, December 19th 2013: Michel Abdalla, David Pointcheval
- PhD: Aurore Guillevic, *Étude de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie*, ENS, December 20th 2013: David Pointcheval, Damien Vergnaud (advisor)

6.4. Invited Talks

6.4.1. At Conferences

- Vadim Lyubashevsky: "The LPN Problem in Cryptography" at the 14th IMA International Conference on Cryptography and Coding. Oxford, UK, December 2013

- David Naccache (common work with Roman Korkikian and Guilherme Ozari de Almeida:): “Instantaneous Frequency Analysis” at SECRYPT 2013, the 10th International Conference on Security and Cryptography. Reykjavik, Iceland, July, 2013
- David Naccache (common work with Eric Brier and Li-yao Xia): “How to Sign Paper Contracts? Conjectures & Evidence Related to Equitable & Efficient Collaborative Task Scheduling” at Open Problems in Mathematical and Computational Sciences Conference, Istanbul, Turkey, September 2013.
- David Naccache (common work with Hervé Chabanne, Jean-Michel Cioranesco, Vincent Despiegel and Jean-Christophe Fondeur) “Using Hamiltonian Totems as Passwords” at SantaCrypt 2013, Prague, Czech Republic, November 2013

6.4.2. At Organized Schools

- Vadim Lyubashevsky: “Lattice-Based Cryptography” at the Ecole de Printemps d’Informatique Theorique. Autrans, France, March 2013
- Vadim Lyubashevsky: “Lattice Cryptography” (5 hour course) at the Summer School on Lattices and FHE at Chongqing University. Chongqing, China, July 2013
- Vadim Lyubashevsky: “Lattice-Based Digital Signatures" at the Workshop on Lattice-Based Cryptography. Bangalore, India, December 2013

6.5. Scientific Animation

6.5.1. Organisation of Events

- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

6.5.2. Steering Committees of International Conferences

- steering committee of CANS: David Pointcheval
- steering committee of PKC: David Pointcheval, David Naccache
- steering committee of FDTC: David Naccache (chair)
- steering committee of PROOFS: David Naccache
- steering committee of LATINCRYPT: Michel Abdalla
- steering committee of PAIRING: Michel Abdalla

6.5.3. Board of International Organizations

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2015), David Pointcheval (2008–2016)

6.5.4. French Research Community

- Recruitment committee at Université of Rennes (PR 27): David Pointcheval
- Recruitment committee at Université of Versailles (MCF 27): Damien Vergnaud
- Recruitment committee at Université Paris 1 (PR 27): David Naccache
- Recruitment committee at Université Paris 2 (MCF 27): David Naccache
- Recruitment committee at Université Paris 2 (MCF 26): David Naccache
- Recruitment committee at École normale supérieure (MCF 27): Damien Vergnaud
- Recruitment committee at École normale supérieure (MCF 27): Damien Vergnaud
- Appointed member of the *Conseil National des Universités* (CNU): Damien Vergnaud
- Scientific board member, Agence pour les mathématiques en interaction avec l’entreprise et la société: David Naccache
- Scientific board member, Conseil supérieur de la formation et de la recherche stratégiques (CSFRS, a French government body): David Naccache
- Qualified Appointee, Banque de France’s Payment Security Observatory: David Naccache

CRYPT Team

6. Dissemination

6.1. Scientific Animation

6.1.1. Editorial Boards

- Advances in Mathematics of Communications: Xiaoyun Wang
- Journal of Cryptology: Phong Nguyen and Xiaoyun Wang
- Journal of Mathematical Cryptology: Phong Nguyen
- Natural Science Review: Xiaoyun Wang

6.1.2. Program Committees of International Conferences

- EUROCRYPT '13 - May, Athens, Greece: Phong Nguyen (Program co-chair)
- ASIACRYPT '13 - December, Bengaluru, India: Phong Nguyen and Xiaoyun Wang

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

PhD: Phong Nguyen, Advanced Cryptanalysis and Lattice Algorithms, 12h, CAS, China

6.2.2. Supervision

PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen

PhD: Yuanmi Chen, Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe, Univ. Paris 7, November 13th 2013, Phong Nguyen

PhD: Aurore Guillevic, Étudie de l'arithmétique des couplages sur les courbes algébriques pour la cryptographie, ENS, December 20th 2013, Damien Vergnaud and Phong Nguyen

PhD: Yupeng Jiang, CAS, Summer 2013, Yingpu Deng

6.2.3. Juries

PhD: Léo Ducas, Signatures fondées sur les réseaux euclidiens: attaques, analyses et optimisations, Univ. Paris 7, November 12th 2013, Phong Nguyen (supervisor)

PhD: Yuanmi Chen, Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe, Univ. Paris 7, November 13th 2013, Phong Nguyen (supervisor)

6.3. Popularization

Phong Nguyen gave several invited talks:

- [17] at the Workshop on Number Theory, Geometry and Cryptography in UK.
- [16] at the Workshop on Algebraic Aspects of Cryptography in Japan.

GEOMETRICA Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorial boards of scientific journals

Jean-Daniel Boissonnat is a member of the Editorial Board of *Journal of the ACM*, *Discrete and Computational Geometry*, *Algorithmica*, *International Journal on Computational Geometry and Applications*.

Frédéric Chazal is a member of the Editorial Board of *SIAM Journal on Imaging Sciences*, *Graphical Models* and *Discrete and Computational Geometry* (start in Jan. 2014).

Olivier Devillers is a member of the Editorial Board of *Graphical Models*.

Monique Teillaud is a member of the Editorial Boards of CGTA, *Computational Geometry: Theory and Applications*, and of IJCGA, *International Journal of Computational Geometry and Applications*.

M. Yvinec is a member of the editorial board of *Journal of Discrete Algorithms*.

Monique Teillaud and Mariette Yvinec are members of the CGAL editorial board.

9.1.2. Conference program committees

Jean-Daniel Boissonnat was a member of the PC of the Symposium on Geometry Processing SGP 2013.

Jean-Daniel Boissonnat chaired WoCG (Workshops in Computational Geometry) and was a member of the program committee of the Young Researchers Forum, two satellite events of the ACM Symposium on Computational Geometry SoCG 2013.

Frédéric Chazal was a member of the PC of the ACM Symposium on Computational Geometry 2013, of the the Scientific committee of the SMAI 2013 conference, and of Geometric Science of Information (GSI 2013).

Monique Teillaud was a member of the PC of EuroCG, the European workshop on computational geometry.

9.1.3. Steering committees

Jean-Daniel Boissonnat is a member of the steering committee of the international conference on Curves and Surfaces.

Monique Teillaud was a member of the Computational Geometry Steering Committee until April.

Monique Teillaud has been a member of the Steering Committee of the European Symposium on Algorithms (ESA) since September.

9.1.4. Inria committees

Jean-Daniel Boissonnat was a member of the recruitment committee of Inria Rhône-Alpes.

Frédéric Chazal was a member of the recruitment committee of Inria Saclay (vice-chair).

Monique Teillaud is a member of the Inria Evaluation Committee.
She was a member of the national Inria DR2 interview committee and the local CR2 interview committee.

Monique Teillaud is a member of the local Committee for Technologic Development.
She was also a member of the local committee for transversal masters.

9.1.5. Other committees

Jean-Daniel Boissonnat is a member of the Conseil de l'AERES (Agence d'Evaluation de la Recherche et de l'Enseignement Supérieur).

9.1.6. Conference organization

- O. Devillers and M. Teillaud coorganized the workshop on Geometric Computing (http://www.acmac.uoc.gr/GC2013/ Heraklion, Greece, January) with Menelaos Karavelas (University of Crete) and Elias Tsigaridas (EPI POLSYS).
- M. Teillaud coorganized the Dagstuhl Seminar on Computational Geometry [38] (http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=13101, March 4-8) with Otfried Cheong (KAIST) and Kurt Mehlhorn (MPI Saarbrücken)
- M. Teillaud coorganized the Dagstuhl Seminar on Drawing Graphs and Maps with Curves [39] (http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=13151, April 8-12) with Stephen Kobourov (University of Arizona) and Martin Nöllenburg (Karlsruhe Institute of Technology)
- O. Devillers organized the workshop of ANR Presage (Valberg, France, June).
- M. Teillaud (chair) and O. Devillers coorganized ALGO 2013, in cooperation with members of EPI ABS and COATI (http://algo2013.inria.fr/. Sophia Antipolis, France, September 2-6). ALGO 2013 combined the European Symposium on Algorithms (ESA) and six more specialized conferences and workshops. There were about three hundred attendees.
- D. Cohen-Steiner organized the 2013 edition of the "Journées de Géométrie Algorithmique" held at the CIRM, Luminy in December http://quentin.mrgt.fr/events/jga2013.html.

9.1.7. Web site

M. Teillaud is maintaining the Computational Geometry Web Pages http://www.computational-geometry.org/, hosted by Inria. This site offers general interest information for the computational geometry community, in particular the Web proceedings of the Video Review of Computational Geometry, part of the Annual Symposium on Computational Geometry.

9.1.8. Geometrica seminar

The seminar featured presentations by the following scientists:

Omri Azencot (Technion) : An Operator Approach to Tangent Vector Field Processing

Mirela Ben Chen (Technion - Israel Institute of Technology) : Can Mean-Curvature Flow be Modified to be Non-singular?

Benjamin Burton (University of Queensland) : Untangling knots using combinatorial optimisation

A. Chiara de Vitis (Pavia) : Geometrical and Topological Descriptors for Protein Structures

C. Couprie (Courant Institute) : Graph-based Variational Optimization and Applications in Computer Vision

J. Demantke (IGN) : Geometric Feature Extraction from LIDAR Point Clouds and Photorealistic 3D Facade Model Reconstruction from Terrestrial LIDAR and Image Data

Kyle Heath (Stanford University) : Image Webs: Discovering and using object-manifold structure in large-scale image collections

N. Mitra (UCL London) : Computational Design Tools for Smart Models Synthesis

P. Machado Manhães de Castro (UFPE, Brasil) : Invariance for Single Curved Manifolds

Natan Rubin (Freie Universität Berlin) : On Kinetic Delaunay Triangulations: A Near Quadratic Bound for Unit Speed Motions

D. Salinas (Gipsa Lab, Grenoble) : Using the Rips complex for Topologically Certified Manifold Learning

Régis Straubhaar (Université de Neuchâtel) : Numerical optimization of an eigenvalue of the Laplacian on a domain in surfaces

Jian Sun (Mathematical Sciences Center, Tsinghua University) : Rigidity of Infinite Hexagonal Triangulation of Plane

Anaïs Vergne (Télécom ParisTech) : Algebraic topology and sensor networks

Yuan Yao (School of Mathematical Sciences, Peking University) : The Landscape of Complex Networks

H. Zimmer (Aachen) : Geometry Optimization for Dual-Layer Support Structures

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Graduate level: Olivier Devillers, *Delaunay triangulation*, 6h, Universidade Federal de Pernambuco, Brasil.

Master : J.D. Boissonnat, D. Cohen-Steiner, M. Yvinec, *Computational Geometric Learning* , 24h, International Master Sophia-Antipolis.

Master : S. Oudot, *Computational Geometry: from Theory to Applications*, 36h, École polytechnique.

Master: Jean-Daniel Boissonnat, Frédéric Chazal, Mariette Yvinec, *Computational Geometric Learning*, 24h, Master MPRI, Paris.

Master: Olivier Devillers and Monique Teillaud, *Algorithmes géométriques, théorie et pratique*, 16h, Master SSTIM-VIM, Université Nice Sophia Antipolis.

Doctorat : Jean-Daniel Boissonnat, Frédéric Chazal, Mariette Yvinec, *Analyse géométrique des données* , 7h, Ecole Jeunes Chercheurs GDR Informatique Mathématique, Perpignan.

9.2.2. Supervision

PhD: Mikhail Bogdanov, Delaunay triangulations of spaces of constant negative curvature, Université de Nice - Sophia Antipolis, December 9, Monique Teillaud.

PhD in progress: Thomas Bonis, Topological persistence for learning, started on December 2013, Frédéric Chazal.

PhD in progress: Mickaël Buchet, Topological and geometric inference from measures, Université Paris XI, started October 2011, Frédéric Chazal and Steve Oudot.

PhD in progress : Ross Hemsley, Probabilistic methods for the efficiency of geometric structures and algorithms, started October 1st 2011, Olivier Devillers.

PhD in progress: Ruqi Huang, Algorithms for topological inference in metric spaces, started on December 2013, Frédéric Chazal.

PhD in progress : Clément Maria, Data structures and Algorithms in Computational Topology, started October 1st, 2011, Jean-Daniel Boissonnat.

PhD in progress : Rémy Thomasse, Smoothed complexity of geometric structures and algorithms, started December 1st 2012, Olivier Devillers.

PhD in progress : Mael Rouxel-Labbé, Anisotropic Mesh Generation, started October 1st, 2013, Jean-Daniel Boissonnat and Mariette Yvinec.

9.2.3. Juries

Jean-Daniel Boissonnat was a member (reviewer) of the HDR defense of Dominique Attali (Univ. Grenoble).

Jean-Daniel Boissonnat was a member (reviewer) of the PhD defense committee of David Salinas (Univ. Grenoble). Steve Oudot was also part of that defense committee.

Jean-Daniel Boissonnat was a member (reviewer) of the PhD defense of Jérémy Espinas (Univ. Lyon).

Frédéric Chazal was a member (reviewer) of the PhD defense of Lucie Druoton (Univ. de Bourgogne).

Frédéric Chazal was a member (reviewer) of the PhD defense of Anaïs Vergne (Telecom Paris).

Olivier Devillers was a member of the HDR defense committee of Nicolas Bonichon (Univ. Bordeaux).

Monique Teillaud was a member of the PhD defense committee of Marcel Roeloffzen, TU Eindhoven, October.

9.2.4. Internships

Thomas Bonis, image and shape classification using persistent homology (F. Chazal)

Claudia Werner, Triangulations on the sphere, Hochschule für Technik Stuttgart (Monique Teillaud)

Arnaud Poinas, Statistical manifold reconstruction (Jean-Daniel Boissonnat)

Sergei Kachanovich, Graph-induced simplicial complex (Jean-Daniel Boissonnat)

Chunyuan Li, Persistence-based object recognition (F. Chazal and M. Ovsjanikov)

Venkata Yamajala, Implementing (and simplifying) the tangential complex (Jean-Daniel Boissonnat)

9.3. Popularization

Jean-Daniel Boissonnat, Au delà de la dimension 3, Caféin Inria Sophia Antipolis.

Jean-Daniel Boissonnat, Geometry Understanding in Higher Dimensions. Conference for the students of ENS Lyon (Inria Sophia Antipolis)

Monique Teillaud, “à quoi sert un triangle ?”, 2x2h, Collège Le Prés des Roures, Le Rouret, in the framework of the national Week of Mathematics.

Steve Oudot was coordinator of the *Photomaton 3d* booth at the *Nuit des chercheurs* event at École polytechnique in September 2013. Marc Glisse, Maks Ovsjanikov, Mickaël Buchet, and Thomas Bonis also participated.

9.4. Participation to conferences, seminars, invitations

9.4.1. Invited Talks

Jean-Daniel Boissonnat gave an invited lecture at the International Symposium on Voronoi Diagrams (St Petersburgh) : on the empty sphere on manifolds. July.

Jean-Daniel Boissonnat gave an invited talk at the Jean-Paul Laumond’s day (on the occasion of his 60th anniversary) : Comprendre la géométrie des données.

Frédéric Chazal gave invited talks at the Workshop on Topological Data analysis, Institute for Mathematics and its Applications, Minneapolis, October 2013; at the Workshop on Topological Methods in Complexity Science, European Conference on Complex Systems satellite conference, Barcelona, September 2013.

9.4.2. Seminars

Members of the project have presented their published articles at conferences. The reader can refer to the bibliography to obtain the corresponding list. We list below all other talks given in seminars, summer schools and other workshops.

Frédéric Chazal, Filtrations et entrelacements : théorie et applications en Analyse Topologique des Données, Séminaire Brillouin, Paris, Dec. 2013.

Frédéric Chazal, Transport de mesures et inférence géométrique, Journées de Contôle et Transport Optimal, Dijon, February 2013.

Frédéric Chazal, Computer Science and Machine Learning Seminar at Carnegie Mellon University, Pittsburg, September 2013.

Frédéric Chazal, Convergence rates for persistence diagrams in Topological Data Analysis, Workshop on Applied and Computational Topology, Bremen, July 2013.

Frédéric Chazal, Inférence géométrique et analyse topologique des données à l'aide de fonctions distance, colloquium de mathématiques, Univ. Paris 6, May 2013.

Olivier Devillers. Qualitative Symbolic Perturbations. Workshop on Geometric Computing. Heraklion. January.

Olivier Devillers. Hyperbolic Delaunay Triangulation, Universidade Federal de Pernambuco. June.

Monique Teillaud. Delaunay Triangulations of Point Sets in Closed Euclidean d-orbifolds. Workshop on Geometric Computing. Heraklion. January.

Monique Teillaud. Delaunay Triangulations of Point Sets in Closed Euclidean d-orbifolds. Meeting of ANR Presage. January.

Monique Teillaud. Curves in CGAL (with Michael Hemmer, University of Technology Braunschweig). Dagstuhl Seminar on Drawing graphs and maps with curves. April.

Monique Teillaud. 3D meshes in CGAL. Mathematics for Industry and Society, French Embassy Berlin. July.

9.4.3. Short scientific visits

Frédéric Chazal, Carnegie Mellon University, Sept. 2013.

Frédéric Chazal, Stanford University, May 2013.

Olivier Devillers and Monique Teillaud, University of Athens, January.

Monique Teillaud, Zuse Institut Berlin, July.

Monique Teillaud, TU Eindhoven, October.

GRACE Project-Team

9. Dissemination

9.1. Scientific Committees

- Daniel Augot is member of the scientific committee of the French *CCA seminar*, held thrice a year in Institut Henry Poincaré.
- Daniel Augot was member of the programm committee of Fq11, the 11th International Conference on Finite Fields and their Applications, Magdeburg, July 22-26, 2013.

9.2. Administrative committees

- Alain Couvreur and Benjamin Smith are elected members of the *Commité de centre* of Inria Saclay.
- Alain Couvreur is *Jeune chercheur référent* for the *Commission de suivi doctoral* of Inria Saclay.
- Daniel Augot is member of the *Conseil de Laboratoire* of the LIX as a team leader.
- François Morain, Julia Pieltant and Benjamin Smith are elected members of the *Conseil de Laboratoire* of the LIX.
- Daniel Augot is head of the *Commission de suivi doctoral* of Inria Saclay.
- Daniel Augot is member of the *Bureau du comité des projets* de l'Inria Saclay–Île-de-France.
- Daniel Augot is member of the *commission scientifique* de l'Inria Saclay–Île-de-France.
- Daniel Augot is member of the *commission formation du labex Digicosme*
- Daniel Augot is member of the *comité de programme* of the Digiteo RTRA.
- Daniel Augot was member of the *comité de sélection pour un maître de conférence* at University of Versailles–Saint-Quentin.
- Benjamin Smith became the (scientific) international correspondent for Inria Saclay.
- Benjamin Smith became a member of Inria's Groupe de Travail "Relations Internationales" du Comité d'Orientation Scientifique et Technologique (COST-GTRI).
- Benjamin Smith is responsible for office assignments at LIX.
- Benjamin Smith was the chair of the LIX/Qualcomm/Carnot fellowship committee.
- François Morain is vice-head of the Département d'informatique of Ecole Polytechnique.
- François Morain represents École polytechnique in the committee in charge of *Mention HPC* in the *Master de l'université Paris Saclay*.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Master: Daniel Augot, "Codes correcteurs d'erreurs et applications à la cryptographie" 13.5h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: Benjamin Smith, Algorithmes arithmétiques pour la cryptologie, 13.5h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: François Morain, Algorithmes arithmétiques pour la cryptologie, 9h (equiv TD), M2, Master Parisien de Recherche en Informatique (MPRI), France

Master: Benjamin Smith, Cryptologie, 18h (equiv TD), M1, École polytechnique, France

Licence: Benjamin Smith, Introduction à l'informatique, 40h (equiv TD), L3, École polytechnique, France

Master: Françoise Levy-dit-Vehel, Introduction à la crytopgraphie, 12h (equiv TD), Mastère spécialisé architecture et sécurité des systèmes d'information, ENSTA ParisTech.

Licence : F. Morain, 10 lectures of 1.5h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique (L2). Responsability of this module (350 students).

Master (M1) : F. Morain, 9 lectures of 1.5h, 3rd year course "cryptology" at École polytechnique.

9.3.2. Supervision

- PhD in progress : Cécile Gonçalves, Algorithmes avancés de calcul de cardinalité pour des courbes intéressantes en cryptologie, 1/10/2011, Benjamin Smith and François Morain.
- PhD in progress: Gwezheneg Robert, Métrique rang et codes de Gabidulin en cacractéristique zéro, 1/10/12, Daniel Augot and P. Loidreau.
- PhD: Alexander Zeh, Algebraic Soft- and Hard-Decision Decoding of Generalized Reed–Solomon and Cyclic Codes, Ulm Universität, 2/09/2013, Daniel Augot and Martin Bossert.

9.3.3. Juries

- Alain Couvreur is member of the Jury of the *Agrégation de Mathématiques*, Options C (computer algebra) and D (computer science).
- Benjamin Smith was an examiner for the PhD of Louise Huot (UPMC, 13/12/2013)
- Benjamin Smith was an examiner for the PhD of Aurore Guillevic (ENS, 20/12/2013)
- Benjamin Smith was a member of the jury for the CNRS Concours IE63 (BAP E), 24-25/10/2013.
- Daniel Augot was examiner for the PhD of Mamdouh Abbara (X, 09/04/2013)
- Daniel Augot was reviewer of the PhD of Mila Tukumuli, (Aix-Marseille University, 13/09/2013)
- Daniel Augot was examiner for the PhD of Lin Sok (Télécom Paristech, 20/09/2013)
- Daniel Augot was examiner and reviewer of Johan Nielsen's PhD (DTU Lyngby, 30/09/2013)
- Daniel Augot was examiner and reviewer of Muhammad Foizul Islam Chowdhury's PhD (Western University Canada, London, Canada, 8/11/2013)
- Daniel Augot was reviewer of Stéphanie Dib's PhD (Aix-Marseille University, 11/12/2013)

9.4. Invitations to seminars and conferences

- Daniel Augot : 14/02/2014, GREYC, Caen. "Les connexions entre le logarithme discret sur les corps finis non premiers et le décodage des codes de Reed-Solomon".
- Daniel Augot was invited to participate to a session Cryptography and Number Theory at 2013 SIAM Conference on Applied Algebraic Geometry, 01-04/08/2013.
- Daniel Augot gave a talk at Dagstuhl Seminar 13351 on coding theory, 25-30/08/2013
- Alain Couvreur gave a talk at the Seminar on Coding Theory and Cryptography common to the universities of Neuchâtel and Zurich. 22/04/2013.
- Benjamin Smith was an invited speaker at the international Workshop on Number Theory at the American University of Beirut, Lebanon, 25-27/04/2013.
- Benjamin Smith gave a talk at AGCT-14, an invitational conference on Arithmetic, Geometry, Cryptography, and Coding Theory, 03-07/06/2013.
- Benjamin Smith gave two lectures on number-theoretic cryptography at the CryptoBG international summer school in Oriahovitsa, Bulgaria, 20-27/07/2013.
- Benjamin Smith gave an invited talk at the PIMS Workshop on Curves and Applications, Calgary, Canada, 19-21/08/2013.
- Benjamin Smith gave visited Microsoft Research, Redmond from 22/08/2013 to 04/09/2013, and gave a talk in their seminar.

- Benjamin Smith gave two lectures at the ECC 2013 summer school on Elliptic Curves for Cryptography in Leuven, Belgium, 11-13/09/2013.
- Benjamin Smith was an invited speaker at ECC 2013 (the 17th annual Elliptic Curve Cryptography workshop) in Leuven, Belgium, 16-18/09/2013.
- F. Morain gave three lectures in the summer school *Number theory for cryptography* in Warwick University, june 2013.

9.5. Popularization

- Alain Couvreur gave a talk at *UniThé ou Café*, a monthly science popularization event dedicated to all the employees of Inria Saclay.
- Daniel Augot presented bit operations, the Hamming code, the one-time pad and a bit of steganography to high school students in Courcouronnes, 10/04/2013.

LFANT Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorships

K. Belabas acts on the editorial board of *Journal de Théorie des Nombres de Bordeaux* since 2005 and of *Archiv der Mathematik* since 2006.

H. Cohen is an editorial board member of *Journal de Théorie des Nombres de Bordeaux*; he is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM)*.

J.-M. Couveignes is a member of the editorial board of the *Publications mathématiques de Besançon* since 2010.

A. Enge is an editor of *Designs, Codes and Cryptography* since 2004.

9.1.2. Invited talks

- J.-M. Couveignes attended the Sémestre Mathématique de Besançon in September 2013 and gave a talk on primality testing.
- J.-M. Couveignes attended GEOCRYPT 2013 in Papeete and gave a talk on genus two curves.
- A. Enge: "Class polynomials for dimension 2", Jahrestagung Computeralgebra, Konstanz, 18–22/03/2013
- A. Enge: "Class polynomials for abelian surfaces", Cryptography and Coding Theory at LIX, 20-21/06
- A. Enge: "Class polynomials for abelian surfaces", Number Theory, Geometry and Cryptography, Warwick, 01-05/07

9.1.3. Conference organisation and programme committees

The third atelier PARI/GP was held at IMB from January 14th to 18th, 2013: http://pari.math.u-bordeaux.fr/Events/PARI2013/. External speakers include Eduardo Friedman (Universidad de Chile), Xavier Roblot (Université Claude Bernard Lyon I), Jürgen Klüners (Universität Paderborn), Pascal Molin (Université Paris 7), Loïc Grenié (Università di Milano-Bicocca), Charles Boyd, Christophe Delaunay (Université de Franche-Comté), François Brunault (ENS Lyon), Philippe Elbaz-Vincent (Grenoble), Denis Simon (Caen).

A. Enge and D. Robert were programme committee members of the *Selected Area in Cryptography* 2013 conference.

9.1.4. Seminar

The following external speakers have given a presentation at the LFANT seminar, see
http://lfant.math.u-bordeaux1.fr/index.php?category=seminar

- Friedrich Panitz (Paderborn), "An algorithm to enumerate quartic fields, after Bhargava."
- Sinai Robins (Nanyang Technological University, Singapore) "Cone theta functions and what they tell us about the irrationality of spherical polytope volumes."
- Achill Schürmann (Universität Rostock) "Exploiting Symmetries in Polyhedral Computations."
- Maike Massierer (University of Basel) "Point Compression for the Trace Zero Variety."
- Christophe Ritzenthaler (Université Aix-Marseille) "Sur la distribution des traces des courbes de genre 3 sur les corps finis."
- David Lubicz (CELAR — Rennes) "Algèbre linéaire sur $\mathbb{Z}_p[[u]]$ et application au calcul de réseaux dans les représentations galoisiennes p-adiques."
- Marie-Françoise Roy (Rennes) "Algorithme diviser pour régner pour les cartes routières."
- Sorina Ionica (ENS Paris) "Algorithms for isogeny graphs".
- Philippe Jaming (imb) "Problème de la phase dans le cadre discret"

9.1.5. Research administration

K. Belabas is the head of the mathematics department of University Bordeaux 1. He also leads the computer science support service ("cellule informatique") of the Institute of Mathematics of Bordeaux and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

He is a permanent invited member of the councils of both the math and computer science department (UFR) and the Math Institute (IMB).

J.-P. Cerri is an elected member of the scientific council of the Mathematics Institute of Bordeaux (IMB) and responsible for the bachelor programme in mathematics and informatics.

Since January 2011, J.-M. Couveignes is involved in the *GDR mathématiques et entreprises* and in the *Agence pour les mathématiques en interaction avec l'entreprise et la société*.

Until October 2013, A. Enge was responsible for the international affairs of Inria–Bordeaux-Sud-Ouest. As such, he was a regular member of the COST-GTRI, the Inria body responsible for evaluating international partnerships. Since October 2013, he heads this committee.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: A. Page, Fondamentaux pour les mathématiques et l'informatique, cours et TD, 18h, L1, Université Bordeaux 1, France;

Licence: A. Page, CPBx Analyse 2, TD, 43h, L2, Université Bordeaux 1, France;

Licence: A. Page, Codes et cryptographie, TD, 13h, L1, Université Bordeaux 1, France;

Master: K. Belabas, Computer Algebra, 90h, M2, Université Bordeaux 1, France;

Licence: J.-P. Cerri, Algèbre 1, cours, 22h, L1, Université Bord eaux 1, France;

Licence: J.-P. Cerri, Algèbre 2, TD, 51h, L2, Université Bordeau x 1, France;

Licence: J.-P. Cerri, Cryptographie et Arithmétique, cours, 24h, L 3, Université Bordeaux 1, France;

Licence: J.-P. Cerri, Algèbre 4, TD, 51h, L3, Université Bordeau x 1, France;

Master: J.-P. Cerri, Arithmétique, cours, 36h, M1, Université Bo rdeaux 1, France;

Master: J.-M. Couveignes, Algorithms for public key cryptograph, 40h, M2, Université Bordeaux 1, France;

Master: J.-M. Couveignes, Algorithms for number fields, 40h, M2, Université Bordeaux 1, France;

Licence: P. Lezowski, Ouverture professionnelle (help to students to look for a suitable Master), 12h, L3, Université Bordeaux 1, France;

Licence : N. Mascot, cours intégré MOSE 1003, 27h, L1, Université Bordeaux 1, France;

Licence : N. Mascot, C2I, TD, 15h, L1, Université Bordeaux 1, France;

Summer school: A. Enge, Complex multiplication of elliptic curves, 6h, PhD, Number Theory for Cryptography, Warwick, 24-28/06;

Summer school: A. Enge, Complex multiplication of elliptic curves, 1.5h, PhD, ECC 2013, Leuven, 11-13/09;

Summer school: A. Enge, Pairings on elliptic curves, 1.5h, PhD, ECC 2013, Leuven, 11-13/09.

9.2.2. Supervision

- K. Belabas, A. Enge

  PhD Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, University Bordeaux

- K. Belabas, J.-M. Couveignes

PhD Nicolas Mascot, *Calcul de représentations galoisiennes modulaires*, University Bordeaux

- K. Belabas, P. Stevenhagen

  PhD Athanasios Angelakis, *Number fields sharing the same abelianized Galois group*, ALGANT, University Bordeaux and University Leiden

  K. Belabas, T. Dokchitser, P. Stevenhagen

  PhD Julio Brau, *Computing Galois representations attached to elliptic curves*, ALGANT, University Bordeaux and University Leiden

- A. Enge, D. Robert

  PhD Enea Milio, *Isogénies entre surfaces abéliennes*, University Bordeaux

9.2.3. Juries

K. Belabas was a member of the committee for

Habilitation defense (and referee) of Emmanuel Hallouin in Toulouse (November 2013).

J.-M. Couveignes was amember of the committees for

Professor position at the Université of Rennes (April 2013).

Professor position at the Université of Papeete(April 2013).

PhD defense of Jean-Gabriel Kammerer in Rennes (May 2013).

PhD defense (and referee) of Razvan Barbulescu in Nancy (december 2013).

PhD defense (and referee) of Emmanuel Fouotsa in Rennes (december 2013).

PhD defense (and referee) of Yvan Boyer in Paris (december 2013).

A. Enge was a member of the committees for

evaluation AERES LIP6, 07–09 January 2013;

evaluation AERES PRISM, 03–04 December 2013.

9.3. Popularisation

P. Lezowski has given a presentation on cryptology to high school students during “Fête de la science”.

POLSYS Project-Team

9. Dissemination

9.1. POLSYS seminar

Our seminar hosted over twenty invited speakers in 2013.
http://www-polsys.lip6.fr/Seminar/index.html

9.2. Scientific Animation

L. Perret was a PC member of Inscrypt'13, PKC'13 and Eurocrypt'14. L. Perret joined the editorial board of Designs, Codes and Cryptography.

L. Perret was invited speaker in the workshop "Computer algebra and polynomials" held on November 25-29, 2013 at the Research Institute for Symbolic Computation, Linz, Austria.

M. Safey El Din was invited speaker at

- the Polynomial Optimisation Program at Newton Institute in Cambridge (UK);
- the conference "Numerical Methods and Efficient Computations" in honor of J.-P. Dedieu, CIRM, France, 2013.
- the International Symposium on Symbolic and Algebraic Computation (ISSAC) [21].

C. Eder and E Tsigaridas were invited speakers in the workshop "Gröbner Bases, Resultants and Linear Algebra" held on 3-6 September 3-6, 2013 at the Research Institute for Symbolic Computation, Hagenberg, Austria.

G. Renault was invited speaker in the *Minisymposium On Coppersmith's Heuristic Algorithm for Finding Roots of Multivariate Polynomials* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/sess/dsp_programsess.cfm?SESSIONCODE=16747).

M. Safey El Din co-organized (with P. Boito, G. Chèze and C. Pernet) the *Journées Nationales de Calcul Formel* in CIRM, France (May, 13-17, 2013) (http://jncf2013.imag.fr/).

M. Safey El Din co-organized (with E. Kaltofen and L. Zhi) the *Minisymposium on Exact Certificates in Nonlinear Global Optimization* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/program.cfm?CONFCODE=AG13).

J.-C. Faugère was invited speaker in the *Computer algebra and polynomials* International Workshop at Linz, Austria (Dec 2013).

J.-C. Faugère was invited speaker in the *Multivariate Polynomial Workshop* at Fukuoka, Japan (Fev 2013).

J.-C. Faugère was invited speaker in the *Groebner bases, resultants and linear algebra Workshop* at Linz, Austria (Sep 2013).

M. Safey El Din and E. Tsigaridas organized the *Minisymposium Algorithms in Real Algebraic Geometry and its Applications* in the *SIAM Conference on Applied Algebraic Geometry* at Colorado State University, USA (August 1–4, 2013) (http://meetings.siam.org/program.cfm?CONFCODE=AG13).

M. Safey El Din is member of the editorial board of Journal of Symbolic Computation.

E. Tsigaridas (in collaboration with O. Devillers, M. Karavelas, M. Teillaud) organized the *Workshop on Geometric Computing, Heraklion*, in Greece, January 21 – 25 2013 (http://www.acmac.uoc.gr/GC2013/).

E. Tsigaridas participated in the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) which was held in June 26-29, 2013 at Northeastern University, Boston, Massachusetts, USA and presented the paper [32].

C. Eder participated in the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) which was held in June 26-29, 2013 at Northeastern University, Boston, Massachusetts, USA and presented the paper [27].

C. Eder was invited in University of Mississippi, Hattiesburg Mississippi (USA) on 25 June 2013 and gave a talk on *Improved Gröbner Basis computation with applications in cryptography*.

J.-C. Faugère has the following editorial activities:

- Associate Editor of Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences (SPRINGER).
- Guest Editor of a special issue of the Journal Of Symbolic Computation (2013) (with L. Perret).

D. Wang has the following editorial activities:

- Editor-in-Chief and Managing Editor for the journal
  Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal
  SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).
- Member of the Editorial Boards for the
  - Journal of Symbolic Computation (published by Academic Press/Elsevier, London),
  - Frontiers of Computer Science (published by Higher Education Press, Beijing and Springer, Berlin),
  - Texts and Monographs in Symbolic Computation (published by Springer, Wien New York),
  - Book Series on Mathematics Mechanization (published by Science Press, Beijing),
  - Book Series on Fundamentals of Information Science and Technology (published by Science Press, Beijing).
- Member of the International Advisory Board for the Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

D. Wang was involved in the organization of the following conferences

- General Co-chair of the
  5th International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS 2013) (Nanning, China, December 11-13, 2013).
- Member of the Program Committee
  - 2nd International Workshop on Hybrid Systems and Biology (HSB 2013) (Taormina, Italy, September 2, 2013),
  - 15th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2013) (Timisoara, Romania, September 23-26, 2013).
- Co-organizer and Program Co-chair
  Second International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2013) (Beijing, China, October 23-25, 2013).
- Member of the Steering Committee
  - International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS)
  - International Symposium on Symbolic Computation in Software Science (SCSS).

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Master : J.-C. Faugère. Cours sur les systemes polynomiaux au MPRI Université Paris 7 Denis Diderot, France

Master : J. Berthomieu, Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Algèbre linéaire et applications, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : L. Perret, 96 heures équivalent TD, niveau M1 et M2, Université Pierre-et-Marie-Curie, France

Master : L. Perret, 96 heures équivalent TD, niveau L2 et M3, Université Pierre-et-Marie-Curie, France.

Master : G. Renault, Cryptologie Avancée, 50 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : G. Renault, Algèbre linéaire et applications, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : G. Renault, Introduction à la Cryptologie, 50 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 35 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

9.3.2. Supervision

PhD : Aurélien Greuet, 5 Dec 2013, [1]. *Optimisation polynomiale et variétés polaires : theéorie, algorithmes et implantations.* University of Versailles Saint-Quentin and Université Pierre et Marie Curie, France. V. Cossart and M. Safey El Din.

PhD : Louise Huot, 13 Dec 2013. *Résolution de systèmes polynomiaux et cryptologie sur les courbes elliptiques.* Université Pierre et Marie Curie, France. J.-C. Faugère, P. Gaudry and G. Renault.

PhD : Jing Yang, 2013. Beihang University, China and North Carolina State University, USA. D. Wang and H. Hong.

PhD : Chenqi Mou, 2013. *Solving polynomial systems over finite fields*. Beihang University, China and Université Pierre et Marie Curie, France. J.-C. Faugère and D. Wang.

- J.-C. Faugère and M. Safey El Din supervise the PhD thesis of T. Verron.
- J.-C. Faugère and G. Renault supervise the PhD thesis of R. Zeitoun.
- J.-C. Faugère and L. Perret supervise the PhD thesis of F. Portzamparc.
- J.-C. Faugère supervises the PhD thesis of J. Svartz.
- J.-C. Faugère supervises the PhD thesis of A. Wallet (jointly with V. Vitse, UJF, Grenoble).
- M. Safey El Din supervises (jointly with D. Henrion, LAAS, Toulouse) the PhD thesis of S. Naldi.

9.3.3. Juries

M. Safey El Din was member of

- the Habilitation Thesis Committee of S. Graillat (UPMC) as an examiner (Dec. 2013) ;
- the PhD Thesis committee of A. Greuet (Univ. Versailles Saint-Quentin) as the PhD advisor (Dec. 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as an examiner (Dec. 2013) ;
- the PhD Thesis committee of C. Mou (UPMC and Beihang Univ.) as president (June 2013) ;
- the PhD Thesis committee of J. Rohal (North Carolina State Univ., USA) as an external examiner (Aug. 2013).

J.-C. Faugère was member of

- the PhD Thesis committee of L. Ducas (ENS Paris) as president (2013) ;
- the PhD Thesis committee of S. Montan (UPMC) as president (2013) ;
- the PhD Thesis committee of A. Greuet (Univ. Versailles Saint-Quentin) as examiner (Dec. 2013) ;
- the PhD Thesis committee of C. Mou (UPMC and Beihang Univ.) as PhD advisor (June 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as PhD advisor (Dec. 2013) ;

M. Safey El Din participated to the hiring committee for promotion to Associate Professor of the Academy of Mathematics and Systems Science in China.

G. Renault was member of

- the PhD Thesis committee of J.-G. Kammerer (Univ. Rennes 1) as examiner (May 2013) ;
- the PhD Thesis committee of L. Huot (UPMC) as PhD advisor (Dec. 2013).

SECRET Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Workshop organization

- *CBC 2013 - the fourth Code-based Cryptography Workshop*, Rocquencourt, June 10-12, 2013. Organizing committee: G. Landais, Rafael Misoczki, N. Sendrier (chair) http://cbc2013.inria.fr/.

8.1.2. Editorial activities

- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *Finite Fields and Their Applications* associate editors: A. Canteaut, P. Charpin.
- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2013, co-editor: A. Canteaut.
- *Finite Fields and Their Applications. Character Sums and Polynomials*, Radon Series on Computational and Applied Mathematics, Degruyter, In Press. Editeurs: P. Charpin, A. Pott (U. Magdeburg) et A. Winterhof (Austrian Acad. of Sc.)
- A. Canteaut serves on the steering committee of *Fast Software Encryption (FSE)*;
- N. Sendrier serves on the steering committee of *Post-quantum cryptography (PQCrypto)*;
- M. Naya-Plasencia serves on the steering committee of the *Coding and Cryptography* group of GDR-IM https://crypto.di.ens.fr/c2:main.

8.1.3. Program committees

- FSE 2013: March 11-13, 2013, Singapore, Singapore (A. Canteaut, M. Naya-Plasencia);
- WCC 2013: April 15-19, 2013, Bergen, Norway (A. Canteaut, N. Sendrier);
- PQCrypto 2013: June 4-7, 2013, Limoges, France (N. Sendrier, JP. Tillich);
- CBC 2013: June, 10-12, 2013, Rocquencourt, France (N. Sendrier, JP. Tillich);
- SAC 2013: August, 14-16, 2013, Vancouver, Canada (A. Canteaut, M. Naya-Plasencia);
- MoCrySEn 2013: September, 2-6, 2013, Regensburg, Germany (N. Sendrier, co-chair; D. Simos, chair; M. Naya-Plasencia, J.P. Tillich);
- Asiacrypt 2013: December 1-5, 2013, Bangalore, India (A. Canteaut, N. Sendrier);
- *IMA International Conference on Cryptography and Coding*: December 17-19, 2013, Oxford, UK (P. Charpin, M. Naya-Plasencia);
- *Optimal Codes and Related Topics - OC 2013*, September 6-8, 2013, Albena, Bulgaria (P. Charpin);
- FSE 2014: March 2-5, 2014, London, UK (A. Canteaut);
- Africacrypt 2014: May, 28-30, 2014, Marrakech, Morocco (M. Naya-Plasencia);
- Eurocrypt 2014: May, 11-15, 2014, Copenhagen, Denmark (M. Naya-Plasencia);
- YACC 2014: June, 9-14, 2014, Porquerolles, France (N. Sendrier, JP. Tillich)
- ACNS 2014: June 10-13, 2014, Lausanne, Switzerland (A. Canteaut);
- SAC 2014: August 14-15, 2014, Montréal, Canada (A. Canteaut, M. Naya-Plasencia);
- Crypto 2014: August 17-21, 2014, Santa Barbara, USA (M. Naya-Plasencia);
- SCN 2014: September 3-5, 2014, Amalfi, Italy (G. Leurent);
- Latincrypt 2014: September, 17-19, 2014, Florianópolis, Brazil (N. Sendrier);

- Asiacrypt 2014: December 7-11, 2014, China (M. Naya-Plasencia);
- Indocrypt 2014: December 14-17, 2014, New Delhi, India (A. Canteaut).

8.1.4. Invited talks

- A. Canteaut, *Extended differential properties of cryptographic functions*, The 11th International Conference on Finite Fields and their Applications - Fq11, Magdeburg, Germany, July 2013.
- A. Canteaut, *Similarities between Encryption and Decryption: How far can we go?* (Stafford Tavares lecture,), Selected Areas in Cryptography - SAC 2013, Vancouver, Canada, August 2013.
- A. Leverrier, *A Combinatorial Approach to Nonlocality and Contextuality*, Quo Vadis, Quantum Physics?, Natal, Brazil, February 2013.
- A. Leverrier, *Security of continuous-variable quantum key distribution against general attacks*, APS March Meeting 2013, Baltimore, United States of America, March 2013.
- N. Sendrier, *The Construction of Code-Based Cryptosystems*, The 14th IMA International Conference on Cryptography and Coding, Oxford, United Kingdom, December 2013.

A. Canteaut and M. Naya-Plasencia have been invited to give a talk to the *Keccak & SHA-3 Day* organized in Brussels, following the selection of the hash function Keccak as the new SHA-3 standard:

- A. Canteaut, *On some algebraic properties of Keccak*, Keccak & SHA-3 Day, Brussels, Belgium, March 2013;
- M. Naya-Plasencia, *First practical results on reduced-round Keccak and Unaligned rebound attack*, Keccak & SHA-3 Day, Brussels, Belgium, March 2013.

The members of the project-team have also been invited to give talks to some workshops or international seminars, including:

- P. Charpin, *On binary* $[2^n - 1, 2^n - 1 - 2n, d]$ *codes*, workshop "Coding Theory", Dagstuhl Seminar 13351, August 2013.
- A. Leverrier. *Does BosonSampling need Fault-Tolerance?*, Journées Informatique Quantique 2013, Nancy, France, October 2013.
- M. Naya-Plasencia, *Meet-in-the-middle through an Sbox*, ESC 2013 - Early Symmetric Crypto seminar, Luxembourg, Luxembourg, January 2013.
- N. Sendrier, *Classical algorithm techniques for decoding generic linear codes*, workshop “Quantum Cryptanalysis”, Dagstuhl Seminar 13371, September 2013.

8.1.5. Other responsibilities in the national community

- N. Sendrier is a vice-chair of the “Commission d’Evaluation” at Inria;
- N. Sendrier served on the following Inria juries: admissibilité DR2, admissibilité CR2 Rennes, admission CR;
- N. Sendrier has served on the selection committee of PEPS IQC (quantum information and communication, CNRS);
- A. Canteaut is a member of the “Comité de pilotage” of the Fondation Sciences Mathématiques de Paris;
- JP. Tillich is in charge of “Formation par la recherche” for the Paris-Rocquencourt Inria center.
- P. Charpin served on the selection committee for postdoctoral positions, Inria Paris-Rocquencourt.
- P. Charpin served on the selection committee for PhD fundings in Computer Science at University Pierre-et-Marie Curie (theme: *Software and Algorithms*).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master: A. Canteaut, *Stream ciphers*, 9 hours, M2, Telecom ParisTech, France;

Master: A. Canteaut, *Introduction to symmetric cryptography*, 4.5 hours, M2, Telecom ParisTech, France;

Master: A. Canteaut, *Error-correcting codes and applications to cryptlogy*, 11 hours, M2, University Paris-Diderot (MPRI), France;

Master: N. Sendrier, *Code-based cryptography*, 4.5 hours, M2, University Paris-Diderot (MPRI), France;

Master: J.-P. Tillich, *Introduction to Information Theory*, 32 h, M2, Ecole Polytechnique, France.

The members of the project-team also gave advanced lectures to several summer schools for PhD students: *Icebreak 2013* (Reykjavik, Iceland, June 2013) [22], [25]; *Summer school on Design and Security of Cryptographic Functions, Algorithms and Devices* (Albena, Bulgaria, June 2013) [31]; *2013 Indian National Workshop on Cryptology* (Delhi, India, October 2013) [33]; *Forum des jeunes mathématicien-ne-s 2013* (Lyon, France, November 2013) [48].

8.2.2. Supervision

PhD: Mamdouh Abbara, *Quantum turbo-codes*, Ecole Polytechnique, April 9, 2013 (supervisor: JP. Tillich)

PhD: Rafael Misoczki, *Two Approaches for Achieving Efficient Code-Based Cryptosystems*, Université Pierre-et-Marie Curie, November 25, 2013 (supervisor: N. Sendrier)

PhD: Jean-Christophe Sibel, *Region-based approximation to solve inference in loopy factor graphs: decoding LDPC codes by the Generalized Belief Propagation*, Université de Cergy-Pontoise, June 7, 2013 (supervisor : D. Declercq)

PhD in progress: Marion Bellard, *Influence du mapping pour la reconnaissance d'un système de communication*, since January 2011, supervisors: N. Sendrier and J.-P. Tillich

PhD in progress: Virginie Lallemand, *Cryptanalysis for symmetric crytography*, since October 2013, supervisors: M. Naya-Plasencia and A. Canteaut

PhD in progress: Grégory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, since October 2010, supervisors: M. Finiasz and N. Sendrier

PhD in progress: Denise Maurice, *Quantum LDPC codes*, since September 2010, supervisor: JP. Tillich

PhD in progress: Joëlle Roué, *Security analysis of block ciphers*, since September 2012, supervisor: A. Canteaut

PhD in progress: Valentin Suder, *Permutations for symmetric cryptography*, since October 2011, supervisor: P. Charpin

PhD in progress: Audrey Tixier, *Reconnaissance de turbo-codes et de codes LDPC*, since October 2013, supervisor: J.P. Tillich

8.2.3. Juries

- Risto Hakala, *Results on Linear Models in Cryptography*, Aalto University, Helsinki, Finlande, February 2013, committee: P. Charpin (reviewer).
- Mohamed Ahmed Abdelraheem, *Cryptanalysis of Some Lightweight Symmetric Ciphers*, Danmarks Tekniske Universitet, Denmark, February 7, 2012, committee: A. Canteaut (reviewer);
- Mamdouh Abbara, *Turbo-codes quantiques*, Ecole Polytechnique, April 9, 2013, committee: JP. Tillich (supervisor);
- Paul Stankovski, Lunds University, Sweden, June 17, 2013, committee: A. Canteaut (opponent);
- Alexander Zeh, *Algebraic Soft- and Hard-Decision Decoding of Generalized Reed–Solomon and Cyclic Codes*, Ecole Polytechnique/University of Ulm, September 2, 2013, committee: P. Charpin (reviewer), JP. Tillich;

- Anne Marin, *Utilisation d'états multigraphes pour le partage de secret quantique*, Télécom ParisTech, September 17, 2013, committee: J.P. Tillich;
- Jérémy Jean, *Cryptanalyse de primitives symétriques basées sur le chiffrement AES*, École Normale Supérieure, September 24, 2013, committee: A. Canteaut (reviewer);
- Rafael Misoczki, *Two Approaches for Achieving Efficient Code-Based Cryptosystems*, University Pierre-et-Marie-Curie, November 25, 2013, committee: N. Sendrier (supervisor), JP. Tillich;
- Julien Schrek, *Signatures et authentification pour les cryptosystèmes basés sur les codes correcteurs en métrique de Hamming et en métrique rang*, University of Limoges, November 27, 2013, committee: N. Sendrier (reviewer), J.P. Tillich;
- Patrick Debrez, *Attaques par Rencontre par le Milieu sur l'AES*, École Normale Supérieure, December 9, 2013, committee: G. Leurent
- Alberto Passuello, *Semidefinite programming in combinatorial optimization with applications to coding theory and geometry*, University of Bordeaux, December 17, 2013, committee: J.P. Tillich

Specfun Team

9. Dissemination

9.1. Scientific Animation

The team started a seminar, first on an irregular basis, but with the view of running more regular sessions. It attracted researchers from teams in the neighbouring environment and had 8 sessions in 2013.

F. Chyzak is part of the scientifique committee of the *Journées Nationales de Calcul Formel*, the annual meeting of the French computer algebra community.

A. Mahboubi and E. Tassi have organized the 5th edition of the Coq international workshop (satellite of the Itp 2013 conference, Rennes, July 2013).

A. Mahboubi has participated to the organization of the Lix Colloquium (November 2013) and of the satellite PSATT international workshop.

A. Mahboubi has served in the program committee of the 5th edition of the Coq international workshop.

A. Mahboubi has served in the program committee of the ITP 2013 international conference.

A. Bostan has served as the Poster Committee Chair for the ISSAC 2013 international conference.

A. Bostan has served in the program committee of the MEGA 2013 international conference.

A. Bostan has served in the program committee of the FPSAC 2013 international conference.

A. Bostan has served in the program committee of the SYNASC 2013 international conference.

A. Bostan is part of the Scientific advisory board of the MEGA conference series.

A. Mahboubi and E. Tassi have given an invited tutorial at the ITP 2013 international conference (Rennes, France).

A. Mahboubi has given an invited talk at the Calculemus 2013 conference (Bath, United Kingdom).

A. Mahboubi has given an invited talk at the Colloquium of the Institute of Mathematics at the University of Nantes (France).

A. Mahboubi has given an invited talk, joint with G. Gonthier at the Dutch Mathematical Congress 2013 (Nijmegen, Netherlands).

A. Mahboubi has given an invited talk at the British Colloquium for Theoretical Computer Sciences (Bath, United Kingdom).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master : A. Bostan, *Algorithmes efficaces en calcul formel*, 12h, M2, MPRI, France
- Master : F. Chyzak, *Algorithmes efficaces en calcul formel*, 12h, M2, MPRI, France
- Master : A. Mahboubi, *Assistants de preuves*, 18h, M2, MPRI, France
- Agrégation de Mathématiques : A. Bostan, *Préparation épreuve de modélisation, option C*, 12h, ÉNS Cachan, France

9.2.2. Supervision

- PhD: B. Morcrette, *Combinatoire analytique et modèles d'urnes*, June 2013, Ph. Flajolet, M. Soria and Ph. Dumas

- PhD in progress: A. Barillec, *Asymptotique automatique certifiée des fonctions spéciales*, September 2013, F. Chyzak and A. Mahboubi
- PhD in progress: L. Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, September 2013, A. Bostan and B. Salvy
- PhD in progress: P. Lairez, *Algorithmique efficace pour la création télescopique, et ses applications*, September 2011, A. Bostan and B. Salvy
- L3: D. Rouhling, ÉNS Lyon, *Proof search modulo a theory in sequent calculus*, June–July 2013, S. Graham-Lengrand (CNRS, LIX) and A. Mahboubi

9.2.3. Juries

- A. Mahboubi has served as examiner in the PhD jury of Mahfuza Farooque, *Automated reasoning techniques as proof-search in sequent calculus*, December 19, 2013.
- A. Bostan has served as examiner in the PhD jury of Basile Morcrette, *Combinatoire analytique et modèles d'urnes*, Université Paris 6, June 26, 2013.

9.3. Popularization

- A. Mahboubi has given a lecture to laureates of the *Olympiades académiques de mathématiques, académie de Créteil*.
  http://maths.ac-creteil.fr/spip/spip.php?article463.
- A. Mahboubi has been involved in the scientific committee for the elaboration of the board game *Mémoire Vive* produced by the Inria communication services.
- A. Mahboubi has given a talk at the forum STIC Paris-Saclay (Palaiseau, France) in November 2013.

VEGAS Project-Team

7. Dissemination

7.1. Scientific Animation

Program and Paper Committee:

- Sylvain Lazard: Program committee of the European Workshop on Computational Geometry (EuroCG'13).

Editorial responsibilities:

- Sylvain Petitjean: Editor of *Graphical Models* (Elsevier).

Workshop organizations:

- Sylvain Lazard co-organized with S. Whitesides (Victoria University) the 12th Inria - McGill - Victoria Workshop on Computational Geometry [3] at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).
- Marc Pouget co-organized the *Journées Informatiques et Géométrie*[4] at Inria Nancy 14-15 Nov.
- Guillaume Moroz organized the session *Calcul formel et numérique* oh the *Rencontres Arithmétiques de l'Informatique Mathématique*[5] at the *Institut Henri Poincaré* Paris 18-20 Nov.

Other responsibilities:

- Sylvain Lazard: Head of the Inria Nancy-Grand Est *PhD and Post-doc hiring committee* (since 2009). Member of the *Bureau du Département Informatique de Formation Doctorale* of the *École Doctorale IAEM* (since 2009). "Chargé de formation par la recherche" for Inria Nancy-Grand Est.
- Laurent Dupont: *Member* of Commission Pédagogique Nationale Infocom/SRC (since 2011). *Member* of Commission Information Scientifique (Inria/Loria).
- Xavier Goaoc: Chair of the Inria *COST-GTRI committee* (2011– august 2013).
- Guillaume Moroz: *Vice delegate* of the *Commission des Utilisateurs des Moyens Informatiques pour la Recherche*.
- Sylvain Petitjean: Director of the Inria Nancy Grand-Est. Member of Inria's *Executive committee*.
- Marc Pouget: Member of the CGAL Editorial Board (since 2008).

[3] Workshop on Computational Geometry
[4] http://jig2013.sciencesconf.org/
[5] http://raim2013.lip6.fr/

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence: Laurent Dupont, *Systèmes de Gestion de Bases de Données Avancé*, 40h, L3, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Concepts et Outils Internet*, 40h, L1, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Programmation Objet et Évènementielle*, 40h, L2, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Rich Internet Applications*, 40h, L2, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont and Yacine Bouzidi, *Programmation de Sites Web Dynamiques*, 70h, L2, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Algorithmique*, 80h, L1, Université de Lorraine (IUT Charlemagne)

Licence: Laurent Dupont *Programmation Objet*, 40h, L1, Université de Lorraine (IUT Charlemagne)

Master: Marc Pouget, *Introduction à la géométrie algorithmique*, 10.5h, M2, École Nationale Supérieure de Géologie, France.

Doctorat: Marc Pouget, *Postdoctoral Summer: Convex hulls and point location*, 15h, IMPA, Rio de Janeiro, Brazil.

Licence: Sylvain Lazard, *Algorithms and Complexity*, 25h, L3, Université de Lorraine.

Licence: Yacine Bouzidi, *Certification informatique et internet*, 54h, L1, Université de Lorraine.

Licence: Yacine Bouzidi, *Langage orienté objet, Java*, 24h, L3, Université de Lorraine.

Licence: Yacine Bouzidi, *Langage d'interrogation des bases de données*, 20h, L3, Université de Lorraine.

7.2.2. Supervision

PhD in progress : Yacine Bouzidi, Résolution de systèmes bivariés et topologie de courbes planes, Oct. 2010, Sylvain Lazard et Marc Pouget.

7.3. Popularization

Guillaume Moroz: Member of the organizing committee of the *Olympiades académiques de mathématiques*.

ALF Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Service to the research community

- Erven Rohou was a member of the program committees of DITAM-PARMA 2014, CC 2014, WPEA 2013.
- Erven Rohou served as an expert for “Région Aquitaine”
- Isabelle Puaut is a member of the program committees of ECRTS 2013, RTNS 2013, RTCSA 2013, RTAS 2014, SIES 2014.
- Isabelle Puaut is member of the Executive Committee (EC) of the IEEE Technical Committee on Real-Time Systems (TCRTS). She is in the steering committee of the ECRTS, RTNS conferences and the WCET workshop.
- Isabelle Puaut is in the management committee of the COST Action TACLe - Timing Analysis on Code-Level (http://www.tacle.eu). She is responsible of Short Term Scientific Missions (STSM) within TACLe. Damien Hardy and Isabelle Puaut participate to TACLe.
- Damien Hardy is a member of the committees of RTNS 2014 and WCET 2014. He was a member of the program committee of WCET 2013, SIES 2013 WIP session and PACT 2013 where he was also the submission chair.
- Pierre Michaud was a member of the program committee of the HPCC 2013 conference.
- André Seznec is a member of the MICRO 2014 top picks committee and a member of SAMOS 2014 program committee.
- André Seznec is a member of the editorial board of the IEEE Micro.
- André Seznec was the Program co-chair of HiPEAC 2013, January 2013
- André Seznec and François Bodin were Program co-chairs of PACT 2013, September 2013.
- François Bodin was a member of ASPLOS 2014, CC 2013, SC 2013 tutorials program committees.
- François Bodin is a member of "Comité de Prospective Scientifique" of the ANR.
- François Bodin is a member of "Conseil Scientifique d’Orap".

9.1.2. Dissemination

- Erven Rohou presented the ANR project W-SEPT at the bi-annual meeting of the “Communauté Française de Compilation”.
- Emmanuel Riou and Nabil Hallou presented the Padrone tool at the HiPEAC Computing Systems Week.
- I. Puaut has presented a seminar on "WCET estimation for multi-core architectures" at LIP6, Paris, in September 2013.
- Damien Hardy, has presented a lesson on "Estimation de pires temps d’exècution (WCET - Worst-Case Execution Times)" at the "école d’été temps-réel" Toulouse, August 2013
- André Seznec presented a keynote entitled "Faster unicores are still needed" at SAMOS XIII in Samos, Greece, July 2013.
- André Seznec presented an invited presentation at Intel Braunschweig in January 2013.
- François Bodin presented invited presentations at the EPOPPEA workshop associated with the HIPEAC 2013 conference, to the CSCI (Comité Stratégique pour le Calcul Intensif), at the HTPC workshop at University of Delaware and at Forum ORAP.

- François Bodin presented a keynote at the HPC languages workshop in Lyon, July 2013
- François presented a lesson at EU ComplexHPC Spring School in Uppsala, June 2013.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master research : A. Seznec, E.Rohou, I. Puaut, F. Bodin, Performance et Microarchitecture, 30 hours, M2, Université de Rennes I, France

Master: A. Seznec, P. Michaud, A. Perais, Architecture des processeurs, 36 hours, M1, Ecole Supérieure d'Ingénieurs de Rennes, France

Master: A. Seznec, P. Michaud, A. Perais, Architecture avancée, 36 hours, M2, Ecole Supérieure d'Ingénieurs de Rennes, France

Master research: I. Puaut, E. Rohou, Rédaction d'articles scientifiques, 28 hours, M2, Université de Rennes I, France

Master research: I. Puaut, Analyse et test formel, 6 hours, M2, Université de Bretagne Occidentale, France

Master: I. Puaut, D. Hardy, Operating systems - process management, 130 hours, M1, Université de Rennes I, France

Master: I. Puaut, Système d'exploitation gestion mémoire, 39 hours, M1, Université de Rennes I, France

Master: I. Puaut, D. Hardy, Systèmes temps-réel, 69 hours, M1, Université de Rennes I, France

Master: F. Bodin, Parallel programming and code optimization, 50 hours, M1, Ecole Supérieure d'Ingénieurs de Rennes, France

Master: F. Bodin, Innovation and technology, 20 hours, M1, Ecole Supérieure d'Ingénieurs de Rennes, France

Master: F. Bodin, Innovation and technology, 40 hours, M1, Université de Rennes I, France

Master: D. Hardy, Systèmes d'exploitation, 44 hours, M1, Université de Rennes I, France

Licence: D. Hardy, Informatique temps-réel, 40 hours, L3, Université de Rennes I, France

9.2.2. Supervision

PhD : J. Lai, Modèle analytique de performance orienté débit d'évaluation de performance des accélérateurs programmables, Université de Rennes I, February 2013. Advisor A. Seznec

PhD : R. Velasquez, Behavioral Application-dependent Superscalar Core Modeling, Université Rennes 1, April 2013. Co-advisors A. Seznec and P. Michaud

PhD : B. Lesage, Architecture multi-coeurs et temps d'exécution au pire cas, Université Rennes 1, May 2013. Co-advisors I. Puaut and A. Seznec

PhD : N. Prémillieu, Améliorer la performance séquentielle à l'ère des processeurs massivement multicoeurs, Université Rennes 1, December 2013. Advisor A. Seznec

PhD in progress: Nabil Hallou, Université Rennes 1, Feb 2013, co-advisors E. Rohou and P. Clauss (EPI Camus Inria Strasbourg)

PhD in progress: Sajith Kalathingal, Université Rennes 1, Dec 2012, co-advisors S. Collange and A. Seznec

PhD in progress: Surya Khizakanchery Natarajan, Université Rennes 1, Jan 2012, advisor A. Seznec

PhD in progress: Hanbing Li, Université Rennes 1, Oct 2012, co-advisors E. Rohou and I. Puaut

PhD in progress: Andrea Mondelli, Université Rennes 1, Oct 2013, co-advisors P. Michaud and A. Seznec

PhD in progress: Bharath Narasimha Swamy, Université Rennes 1, Sept 2011, advisor A. Seznec

PhD in progress: Arthur Perais, Université Rennes 1, Sept 2012, advisor A. Seznec

PhD in progress: Aswinkumar Sridharan, Université Rennes 1, Oct 2013, advisor A. Seznec

PhD in progress: Arjun Suresh , Université Rennes 1, Dec 2012, co-advisors E. Rohou and A. Seznec

9.3. Popularization

- Erven Rohou gave a talk at the SFGP (Société Française du Génie des Procédés): “Stratégies d’augmentation des performances de calcul des logiciels”
- Isabelle Puaut and Erven Rohou gave a lecture at Lycée Descartes: “Les mathématiques au service de la performance des ordinateurs”.

9.4. Miscelleanous

- Erven Rohou co-advised a MSc. student at the Egypt-Japan University of Science and Technology.
- Erven Rohou was a member of the working group GTInria2020 whose mission was to produce the next “Plan Stratégique”.
- Erven Rohou is a member of the Inria CDT (Commission du Développement Technologique)
- As “correspondant scientifique des relations internationales” for Inria Rennes Bretagne Atlantique, Erven Rohou is a member of the Inria COST GTRI (Groupe de Travail "Relations Internationales" du Comité d’Orientation Scientifique et Technologique).
- Erven Rohou served as an expert for “Région Aquitaine”
- A. Seznec is an elected member of the scientific committee of Inria.
- A. Seznec has been nominated by ACM for 3 years 2011-2013 on the selection committee for the ACM-IEEE Eckert-Mauchly award.
- F. Bodin has participated to the Allistene committee on "Préparation de la Stratégie Nationale de Recherche pour le Numérique".
- F. Bodin is a member of the Advisory board of the LPGPU European Project.

ATEAMS Project-Team

7. Dissemination

7.1. Scientific Animation

- Jan van Eijck : Member of the NWO committee “Vrije Competitie” for Computer Science.
- Jan van Eijck : Member of the Advisory Board (‘Raad van Advies’) of the Artificial Intelligence Curriculum, University of Groningen (since Summer 2013).
- Jan van Eijck : Program committee Tenth International Conference on Computational Semantics (IWCS) University of Potsdam, Germany, March 2013
- Jan van Eijck : Program committee LORI-4 (4th International Workshop on Logic, Rationality and Interaction),
- Jan van Eijck : Program committee TTNLS-2014 (Type Theory for Natural Language Semantics)
- Jan van Eijck : Editor of Journal of Logics and their Applications (new IfCoLog journal with open access, to be published by College Publications).
- Jan van Eijck : Reviewer Artificial Intelligence
- Jan van Eijck : Reviewer ESSLLI
- Jan van Eijck : Reviewer Journal of Semantics,
- Jan van Eijck : Reviewer Journal of Logic and Computation
- Jan van Eijck : Reviewer Fundamenta Informaticae
- Jan van Eijck : Reviewer Synthese,
- Jan van Eijck : Reviewer Journal of Philosophical Logic
- Jan van Eijck : Reviewer Journal of Logic Language and Information
- Jan van Eijck : Reviewer Cambridge University Press
- Jan van Eijck : Reviewer Studia Logica.
- Mark Hills : Program committee Working Conference on Reverse Engineering (WCRE/CSMR) Tool-track
- Mark Hills : Reviewer International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)
- Mark Hills : Program committee CALCO Tools
- Paul Klint : Editor Science of Computer Programming
- Paul Klint : Editor Springer Service Science Book Series
- Paul Klint : Visiting Professor University of London, Royal Holloway
- Paul Klint : Treasurer European Association for Programming Languages and Systems (EAPLS)
- Paul Klint : Steering committee member ETAPS
- Paul Klint : Board member Instituut voor Programmatuur en Architectuur (IPA)
- Paul Klint : External advisor PlanComps project (UK)
- Paul Klint : Full Professor at UvA, Software Engineering Chair
- Paul Klint : Director Master Software Engineering, UvA
- Paul Klint : Program committee Software Language Engineering (SLE)
- Paul Klint : Program committee Scalable Language Specifications (SLS 2013)
- Paul Klint : Program committee WasDETT 2013

- Paul Klint : Program committee CSMR WCRE ERA 2014
- Paul Klint : EAPLS PhD Awards 2013
- Atze van der Ploeg : Reviewer Journal of Universal Computer Science
- Tijs van der Storm : Program committee International Workshop on Advanced Software Development Tools and Techniques - (WASDeTT)
- Tijs van der Storm : Program committee International Conference on Generative Programming: Concepts & Experiences (GPCE)
- Tijs van der Storm : Program committee Working Conference on Reverse Engineering (WCRE/CSMR) Tool-track
- Tijs van der Storm : Reviewer ACM Conference on Object-Oriented Programming Systems, Languages and Applications (OOPSLA)
- Tijs van der Storm : Reviewer ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)
- Tijs van der Storm : Member working group IFIP TC2 WGLD 2.16: Working Group on Language Design
- Tijs van der Storm : Reviewer Science of Computer Programming
- Tijs van der Storm : Reviewer Journal of Systems and Software
- Tijs van der Storm : Co-organizer Lorentz Workshop on Language Interaction Design (LIXD)
- Tijs van der Storm : Co-organizer 1st Dutch Conference on Software Development Automation (SDA'13)
- Tijs van der Storm : Co-organizer CWI Scientific Meetings
- Tijs van der Storm : Organizer Normalized Systems Seminar
- Jurgen Vinju : Member steering committee IEEE International Workshop on Source Code Analysis and Manipulation (SCAM)
- Jurgen Vinju : General Chair IEEE International Workshop on Source Code Analysis and Manipulation (SCAM)
- Jurgen Vinju : Observer IFIP TC2 Working Group 2.3 Programming Methodology
- Jurgen Vinju : Program chair International Workshop on Advanced Software Development Tools and Techniques - (WASDeTT)
- Jurgen Vinju : Program committee International Conference on Model Transformation - (ICMT)
- Jurgen Vinju : Program committee chair WCRE/CSMR Tool Track
- Jurgen Vinju : Organizer International Workshop on Parsing@SLE
- Jurgen Vinju : Program committee WCRE/CSMR ERA track
- Vadim Zaytsev : Steering committee Seminar Series on Advanced Techniques & Tools for Software Evolution (SATToSE)
- Vadim Zaytsev : Program commitee Software Quality Management (SQM)
- Vadim Zaytsev : Program commitee IEEE International Workshop on Source Code Analysis and Manipulation (SCAM)
- Vadim Zaytsev : Program commitee Extreme Modeling Workshop (XM)
- Vadim Zaytsev : Judging commitee ACM Student Research Competition
- Vadim Zaytsev : Program committee co-chair Working Conference on Reverse Engineering (WCRE/CSMR) Tool-track
- Vadim Zaytsev : Reviewer Science of Computer Programming
- Vadim Zaytsev : Workshop co-chair Open and Original Problems in Software Language Engineering (OOPSLE)

- Vadim Zaytsev : Social media co-chair ACM/IEEE 17th International Conference on Model Driven Engineering Languages and Systems (MoDELS)
- Vadim Zaytsev: Colloquium organiser of Programming Environment Meetings (PEM)

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Master : Jurgen Vinju, Paul Klint, Software Evolution, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Tijs van der Storm, Jurgen Vinju, Software Construction, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Jan van Eijck, Bert Lisser, Vadim Zaytsev, Software Testing, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Jan van Eijck, Functional Algorithm Specification, 6 EC, Universiteit van Amsterdam, The Netherlands

7.2.2. Supervision

PhD in progress : Paul Griffioen, Next Generation Computational Auditing, started 2011, supervisors Paul Klint, Philip Elsas

PhD in progress : Anastasia Izmaylova, A General Language Parametric Framework for Software Refactoring, started 2011, supervisors Paul Klint, Jurgen Vinju

PhD in progress : Jeroen van den Bos, Digital Forensics Software Engineering, started 2010, supervisors Paul Klint, Tijs van der Storm

PhD in progress : Atze van der Ploeg, Rapid Language Parametric Prototyping of Software Visualization and Exploration, started 2011, supervisor Paul Klint, Tijs van der Storm

PhD in progress : Davy Landman, Recovery and Synthesis of Domain Specific Language Design, started 2011, supervisors Jurgen Vinju, Paul Klint, supervisors Jurgen Vinju .

PhD in progress : Riemer van Rozen, Software Engineering Principles for the Gaming Domain, started 2011, supervisor Paul Klint, Tijs van der Storm

PhD in progress : Ali Afroozeh, Ambiguity and Disambiguation for Context-free Grammars, started 2012, supervisor Jurgen Vinju

PhD in progress : Pablo Inostroza Valdera, Rich UIs for Domain-Specific Languages, started 2013, supervisor Tijs van der Storm

PhD in progress : Ashim Shahi, Principled Quality Assessment of Software, started 2012, supervisor Paul Klint, Jurgen Vinju

PhD in progress : Michael Steindorfer, Scaling meta-programming to data-programming, started 2012, supervisor Paul Klint, Jurgen Vinju

Paul Klint, Jurgen Vinju, Tijs van der Storm, Mark Hills, Jeroen van den Bos and Jan van Eijck together also supervised more than 30 master thesis projects for Universiteit van Amsterdam in 2013.

7.2.3. Juries

- Jan van Eijck, PhD: Arno Bastenhof, Universiteit Utrecht, The Netherlands
- Jan van Eijck, PhD: Frédéric Moisan, Université de Toulouse, France
- Paul Klint, Phd: Romulo Goncalvez, Universiteit van Amsterdam, The Netherlands
- Jurgen Vinju, PhD: C.P.T. de Gouw, Universiteit Leiden, The Netherlands.

7.3. Popularization

- Jan van Eijck : “Why Learn Haskell?”, Talk for UvA Programming Summer School, Amsterdam, July 2, 2013.
- Paul Klint, Davy Landman: “Hoe ontstond de eerste computer?” (“The origin of the first computer”), Public lecture for broad audience, NEMO, Amsterdam.
- Paul Klint, “How to test a meta-program?”, invited talk at the Workshop on Scalable Language Specification (SLS 2013).
- Paul Klint, "BaMa: Key to the Future?", invited talk at IW1010: 10 Years of UvA Information Sciences, Amsterdam
- Paul Klint, “Understanding the Quality of Open Source Projects”, invited talk at SATToSe, Bern
- Davy Landman : “What Does Control Flow Really Look Like? Eyeballing the Cyclomatic Complexity Metric”, poster and presentation at ICT.OPEN (NWO networking event).
- Michael Steindorfer : “Object Redundancy Profiling in Java”, poster and presentation at ICT.OPEN (NWO networking event).
- Tijs van der Storm : “Domain-specific languages”, Guest lecture Bachelor Computer Science, Universiteit van Amsterdam
- Tijs van der Storm : “Opportunities and Risks of MDD – The case of Derric: a DSL for digital forensics”, Presentation at CodeGeneration 2013.
- Tijs van der Storm : “Implementing Domain-specific languages using Rascal”, Invited Presentation at Sioux: Source of your technology.
- Tijs van der Storm, Kevin van der Vlist, Jimi van der Woning : “Questionnaires in Rascal”, participation Language Workbench Challenge 2013 (LWC’13).
- Tijs van der Storm, Alex Loh, “Questionnaires in Ensō”, participation Language Workbench Challenge 2013 (LWC’13).
- Tijs van der Storm : “QL: a language for questionnaires”, assignment description LWC’13.
- Tijs van der Storm : “Software Development Automation Research: Collaboration with Industry”, presentation at the 1st Dutch conference on Software Development Automation (SDA’13).
- Jurgen Vinju : “Modularity”, Guest lecture Bachelor Computer Science, Universiteit van Amsterdam
- Jurgen Vinju : “Software Analysis and Transformation with Rascal” , Presentation NBIC BioAssist meeting (BioAssist)
- Jurgen Vinju, Tijs van der Storm, Atze van der Ploeg, Anastasia Izmaylova, Ali Afroozeh : CWI Open Day, demonstration of NAO robot programming to children using dedicated DSL “Marvol”.
- Jurgen Vinju, Tijs van der Storm, Atze van der Ploeg : “CWI In Bedrijf” (CWI and Industry) , demonstration of Rascal language workbench using the NAO robot DSL “Marvol”.
- Vadim Zaytsev : “A Snappy Introduction to Metaprogramming in Rascal”, RedDevCon’13.
- Vadim Zaytsev : “Modeling Software Structures with GrammarLab”, Tutorial at MoDELS’13.

CAIRN Project-Team

8. Dissemination

8.1. Scientific Animation

O. Berder was General Chair of the 3rd Workshop on Ultra Low Power Systems (WUPS), Prague, Czech Republic, February 2013.

D. Chillet was member of the technical program committee of HiPEAC RAPIDO, HiPEAC WRC, DCIS, and DASIP.

M. Gautier was a member of the technical program committe of IEEE WCNC 2013, IEEE PIMRC 2013, IEEE Percom 2013 (Workshop on Cognitive Computing and Communications), IEEE ICCVE 2013 and IARIA COCORA 2013.

A. Tisserand was a member of technical program committee of the following conferences: IEEE ARITH'21, IEEE Reconfig 2013, DASIP 2013, IEEE NEWCAS 2013. He is a member of the editorial board of the International Journal of High Performance Systems Architecture, Inderscience.

C. Wolinski was a member of the technical program committee of IEEE ASAP and DSD.

F. Charot, O. Sentieys and A. Tisserand are members of the steering committee of a CNRS spring school for graduate students on embedded systems architectures and associated design tools (ARCHI).

O. Sentieys and A. Tisserand are members of the steering committee of a CNRS spring school for graduate students on low-power design (ECOFAC).

A. Tisserand co-organized the ARCHI 2013 école thématique CNRS Architectures des systèmes matériels enfouis et méthodes de conception associées, March 25-29 Col-de-Porte. Details on http://tima-sls.imag.fr/archi13

A. Tisserand was Editor of a special issue in Journal TSI (Technique et Science Informatique) [81].

O. Sentieys was a member of technical program committee of the following conferences: IEEE/ACM DATE, IEEE FPL, ACM/IEEE MEMOCODE IEEE VTC, IEEE DDECS, ACM SBCCI, FTFC. He was Track Chair at IEEE NEWCAS. He is on the editorial board of Journal of Low Power Electronics, American Scientific Publishers, and of ISRN Sensor Networks.

O. Sentieys is a member of the steering committee of the GDR SOC-SIP. He is the chair of the IEEE Circuits and Systems (CAS) French Chapter. In 2013, he was an expert for some scientific organizations (ANR, AERES).

O. Berder is an elected member of IRISA Lab Council. He is the moderator of the Embedded Systems area in the Scientists Interest Group on Intelligent Transportation Systems.

E. Casseau was an expert for the ANR INS program (Agence Nationale de la Recherche).

8.2. Seminars and Invitations

A. Tisserand gave an invited lecture at the CNRS ARCHI 2013 spring school on FPGA circuits.

A. Tisserand gave an invited lecture at the ARIC team of LIP Laboratory, ENS Lyon, on Arithmetic Level Countermeasures for ECC Cryptoprocessors Against Side Channel Attacks.

8.3. Teaching - Supervision - Juries

8.3.1. Teaching Responsibilities

There is a strong teaching activity in the CAIRN team since most of the permanent members are Professors or Associate Professors.

C. Wolinski is the Director of ESIR.
P. Quinton is the director of Ecole Normale Supérieure de Rennes.
D. Chillet is the Director of Academic Studies of ENSSAT.
P. Scalart is the Head of the Electronics Engineering department of ENSSAT.
S. Derrien is the responsible of the first year of the master of computer science at ISTIC since Sep. 2012.
O. Sentieys is responsible of the "Embedded Systems" branch of the SISEA Master of Research (M2R).
D. Chillet is the co-repsonsible of the Embedded System speciality of the ICT Master of University of Science and Technology of Hanoi.

ENSSAT stands for *"École Nationale Supérieure des Sciences Appliquées et de Technologie"* and is an *"École d'Ingénieurs"* of the University of Rennes 1, located in Lannion.
ISTIC is the Electrical Engineering and Computer Science Department of the University of Rennes 1.
ESIR stands for *"École supérieure d'ingénieur de Rennes"* and is an *"École d'Ingénieurs"* of the University of Rennes 1, located in Rennes.
M2R stands for Master by Research, second year.

D. Chillet is member of the French National University Council since 2009 in signal processing and electronics (Conseil National des Universités en 61e section).
D. Chillet is member of the Permanent Committee of the French National University Council since november 2011 in signal processing and electronics (Commission Permanente du Conseil National des Universités en 61e section).
A. Tisserand is member of the French National University Council since 2011 in computer science (Conseil National des Universités en 27e section).

8.3.2. Teaching

O. Berder: introduction to signal processing, 38h, ENSSAT (L3)

O. Berder: microprocessors and digital systems, 30h, ENSSAT (L3)

O. Berder: wireless communications, 23h, ENSSAT (M2)

O. Berder: ad hoc networks, 58h, ENSSAT (M1-M2)

O. Berder: signal processing, 12h, IUT Lannion (L2)

E. Casseau: signal processing, 16h, ENSSAT (L3)

E. Casseau: low power design, 6h, ENSSAT (M1)

E. Casseau: real time design methodology, 24h, ENSSAT (M1)

E. Casseau: computer architecture, 36h, ENSSAT (M1)

E. Casseau: system on chip and verification, 10h, Master by Research and ENSSAT (M2)

E. Casseau: reconfigurable architectures, 25h, USTH (M2)

S. Derrien: component and system synthesis, 16h, Research Master (MRI ISTIC) (M2)

S. Derrien: computer architecture, 12h, ENS Cachan (L3)

S. Derrien: introduction to operating systems, 8h, ISTIC (M1)

F. Charot: specification of applications with the signal synchronous language, 24h, ESIR (M1)

F. Charot: virtual prototyping of multiprocessor system-on-chip, 24h, ESIR (M1)

F. Charot: design of embedded systems, 28h, ESIR (M1)

A.Courtay: Processor Architecture, 24h, ENSSAT (L3)

A.Courtay: Digital Electronics, 32h, ENSSAT (L3)

A.Courtay: Digital System Design, 12h, ENSSAT (L3)

A.Courtay: Digital Electronics Communication Interfaces, 68h, ENSSAT (M1)

A.Courtay: Processor Architecture, 25h, USTH (M1)

D.Chillet: Basic processor architecture, 20h, ENSSAT (L1)

D.Chillet: Design methodology of real-time systems, 32h, ENSSAT (L2)

D.Chillet: Advanced processor architectures, 24h, ENSSAT (M2)

D.Chillet: Multimedia processor architectures, 24h, ENSSAT (M2)

D.Chillet: Multi-processor systems, 20h, ENSSAT (M2)

D. Chillet: advanced processors architectures, 24h, Master by Research and ENSSAT (M2)

D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne and University of Occidental Brittany (UBO) (M2)

D. Chillet: Digital system design, 25h, University of Science and Technology of Hanoi (M1)

D. Chillet: Advanced Multiprocessor system , 25h, University of Science and Technology of Hanoi (M2)

M.Gautier, electronics, 42h, IUT Lannion (L1)

M.Gautier, telecommunications, 114h, IUT Lannion (L1)

M.Gautier, digital communications, 28h, IUT Lannion (L2)

C. Killian, digital electronics, 74h, IUT Lannion (L1)

C. Killian, digital electronics, 28h, IUT Lannion (L2)

C. Killian, electricity, 60h, IUT Lannion (L1)

C. Killian, signal processing, 40h, IUT Lannion (L2)

R. Rocher: electricity, 16h, IUT Lannion (L1)

R. Rocher: electronics, 44h, IUT Lannion (L1)

R. Rocher: telecommunications, 82h, IUT Lannion (L1)

R. Rocher: signal processing, 12h, IUT Lannion (L2)

R. Rocher: digital communications, 48h, IUT Lannion (L2)

P. Scalart: non-linear optimisation, 18h, Master by Research and ENSSAT (M2)

P. Scalart: Parametric modelisation, optimal and adaptive Filters, 24h, Master by Research and ENSSAT (M2)

P. Scalart: source coding, 14h, Master by Research and ENSSAT (M2)

P. Scalart: cellular networks, 24h, ENSSAT (M2)

P. Scalart: digital communication systems, 32h, ENSSAT (M1)

P. Scalart: random signals and systems, 12h, ENSSAT (M1)

O. Sentieys: digital signal processing, 40h, ENSSAT (M1)

O. Sentieys: VLSI integrated circuit design, 40h, ENSSAT(M1)

A. Tisserand: multiprocessor architectures and programming, 20h, ENSSAT and Master by Research, Univ. Rennes 1(M2)

A. Tisserand: hardware computer arithmetic operators, 6h, Master by Research, Univ. Rennes 1 (M2)

C. Wolinski: architecture 1, 64h, ESIR (L3)

C. Wolinski: architecture 2, 28h, ESIR (L3)

C. Wolinski: design of embedded systems, 48h, ESIR (M1)

C. Wolinski: signal, image, architecture, 26h, ESIR (M1)

C. Wolinski: programmable architectures, 10h, ESIR (M1)

C. Wolinski: component and system synthesis, 10h, Master by Research (MRI ISTIC) (M2)

8.3.3. Supervision

PhD: Mahtab Alam, Power Aware Adaptive Techniques for Wireless Sensor Networks, Univ. Rennes 1, Jan. 2013, O. Sentieys, O. Berder, D. Menard.

PhD: Robin Bonamy, Power Consumption Modelling and Optimisation for Heterogeneous Reconfigurable Platform, Univ. Rennes 1, Jul. 2013, D. Chillet.

PhD: Thomas Chabrier, Arithmetic recodings for ECC cryptoprocessors with protections against side-channel attacks, Univ. Rennes 1, Jun. 2013, A. Tisserand, E. Casseau.

PhD: Hervé Yviquel, From dataflow-based video coding tools to dedicated embedded multi-core platforms, Univ. Rennes 1, Oct. 2013, E. Casseau.

PhD: Antoine Morvan, Polyhedral Model for High-Level Synthesis of Pipelined Architectures, Univ. Rennes 1, Jun. 2013, P. Quinton, S. Derrien.

PhD: Vivek D. Tovinakere, Ultra-Low Power Reconfigurable Controllers for Wireless Sensor Networks, Univ. Rennes 1, Feb. 2013, O. Sentieys.

PhD in progress: Florent Berthier, Study and Design of an Ultra Low Power Asynchronous Core for Sensor Networks, Oct. 2013, O. Sentieys, P. Vivet, E. Beigne.

PhD in progress: Karim Bigou, RNS Hardware Units for ECC, Oct. 2011, A. Tisserand.

PhD in progress: Franck Bucheron, Secure Virtualization for Embedded Systems, Oct. 2011, A. Tisserand.

PhD in progress: Aymen Chakhari, Analytical approach for decision errors in fixed-point digital communication systems, Oct. 2010, R. Rocher, P. Scalart.

PhD in progress: Gaël Deest, Computing with Errors: Error-Tolerant Machine Code Generation for Unreliable Embedded Hardware, Oct. 2013, S. Derrien, O. Sentieys.

PhD in progress: Amine Didioui, Reconfigurable Radio Front-End for Energy-Harvesting Wireless Sensor Networks, Nov. 2010, O. Sentieys, C. Bernier.

PhD in progress: Ali Hassan El-Moussawi, Performance/Accuracy Trade-Off in Automatic Parallelization for Embedded Many-Core Platforms, Nov. 2012, S. Derrien.

PhD in progress: Christophe Huriaux, Embedded reconfigurable hardware accelerators with efficient dynamic reconfiguration management, Oct. 2012, O. Sentieys, A. Courtay.

PhD in progress: Quang-Hai Khuat, Real-Time Spatio-Temporal Task Scheduling on 3D Architectures, Oct. 2011, D. Chillet.

PhD in progress: Trong-Nhan Le, Global power management system for self-powered autonomous wireless sensor nodes, Jan. 2011, O. Sentieys, O. Berder.

PhD in progress: Quang-Hoa Le, Virtualized dynamic reconfiguration for 3D SoC, Oct. 2012, E. Casseau, A. Courtay.

PhD in progress: Xuan Chien Le, Indirect Monitoring in Self-Powered Wireless Sensor Networks for Smart Grid and Building Automation, Oct. 2013, O. Sentieys, O. Berder.

PhD in progress: Jérémie Métairie, Reconfigurable Arithmetic Units for Secure Cryptoprocessors, Oct. 2012, A. Tisserand, E. Casseau.

PhD in progress: Van Thiep Nguyen, Energy-efficient MAC protocols for cooperative strategies in Wireless Sensor Networks, Oct. 2013, O. Berder, M. Gautier.

PhD in progress: Viet-Hoa Nguyen, Energy-efficient cooperative techniques for Wireless Body Area Sensor Networks, Nov. 2012, O. Berder, jointly with C. Langlais from Telecom Bretagne.

Ganda-Stéphane Ouedraogo, Automatic synthesis of hardware accalerator from high-level specifications in flexible radios, Oct. 2011, M. Gautier, O. Sentieys.

PhD in progress: Rengarajan Ragavan, Ultra-Low Power Reconfigurable Architectures for Computing and Control in Wireless Sensor Networks, Oct. 2013, O. Sentieys, C. Killian.

PhD in progress: Mai-Thanh Tran, Hardware Synthesis of Flexible and Reconfigurable Radio from High-Level Language Dedicated to Physical Layer of Wireless Systems, Oct. 2013, E. Casseau, M. Gautier.

PhD in progress: Pramod P. Udupa, Sampling, synchronising, digital processing and FPGA implementation of 100Gbps optical OFDM signals, Jan. 2011, O. Sentieys.

PhD in progress: Zhongwei Zheng, Short-range geolocation algorithms based on distributed multi-sensor processing, Nov. 2012, P. Scalart, jointly with C. Roland from Lab-STICC.

8.4. Popularization

A popularisation paper on energy efficiency has been published in [80]
15 members of the team participated in the national science festival (Fête de la Science) in Plemeur-Bodou in October (demonstrations on wireless sensor networks, cryptology and digital integrated circuits).

A letter was published in Inria Emergences on "improving energy efficiency of embedded processors": http://emergences.inria.fr/lettres2013/newsletter-n28/L28_GECOS

CAMUS Team

9. Dissemination

9.1. Scientific Animation

Philippe Clauss, Cédric Bastoul and Vincent Loechner have been part of the program committee of IMPACT 2013 and IMPACT 2014 workshops (International Workshop on Polyhedral Compilation Techniques), held in conjunction with the international conferences HiPEAC 2013 and HiPEAC 2014.

Cédric Bastoul has been co-organizing the HIP3ES 2014 workshop (High Performance Energy Efficient Embedded Systems) held in conjunction with the international conference HiPEAC 2014. Vincent Loechner has been part of its program committee.

Cédric Bastoul is part of the program committee of PARMA+DITAM 2014 (5th Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures 3rd Workshop on Design Tools and Architerctures for Multicore Embedded Computing Platforms), Vienna, Austria.

Cédric Bastoul has been part of the program committee of PACT 2013 (International Conference on Parallel Architecture and Compilation Techniques), Edinburg, Scotland.

Cédric Bastoul has been part of the program committee of PARMA 2013 (Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures), Berlin, Germany.

Philippe Clauss has been part of the program committee of the MSPC 2013 workshop (Memory Systems Performance and Correctness) held in conjunction with the international conference PLDI 2013, Seattle, USA.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Philippe Clauss did not teach in 2013 since he was detached at Inria during the whole year (*délégation*). Alain Ketterlin had teaching activities during the first semester of 2013, while he was detached in the Inria team ALF in Rennes during the second semester.

Licence : Cédric Bastoul, Operating Systems, 30h, L2, Paris-Sud University, France
Licence : Cédric Bastoul, Information Security, 8h, L3, Paris-Sud University, France
Licence : Cédric Bastoul, Networks, 60h, L2, Paris-Sud University, France
Licence : Cédric Bastoul, System Programming, 28h, L2, Strasbourg University, France
Licence : Cédric Bastoul, Network Programming, 42h, L2, Strasbourg University, France
Master : Cédric Bastoul, Compilation, 72h, M1, Strasbourg University, France
Master : Cédric Bastoul, Parallelism, 13h, M2, Strasbourg University, France
Licence : Éric Violard, Functional Programming, 42h, L2, Strasbourg University, France
Licence : Éric Violard, Computer Architectures, 21h, L2, Strasbourg University, France
Licence : Éric Violard, Algorithms and Data Structures, 37h, L2, Strasbourg University, France
Master : Éric Violard, Compiler Design, 57h, M1, Strasbourg University, France
Master : Éric Violard, Semantics, 48h, M1, Strasbourg University, France
Licence : Vincent Loechner, System Programming, 15h, L2, Strasbourg University, France
Licence : Vincent Loechner, Operating Systems, 28h, L2, Strasbourg University, France
Master : Vincent Loechner, Python Programming, 42h, M1, Strasbourg University, France
Master : Vincent Loechner, Real-time Programming, 22h, M1, Strasbourg University, France
Master : Vincent Loechner, Parallelism, 41h, M1, Strasbourg University, France
Master : Vincent Loechner, Parallel Programming, 52h, M2, Strasbourg University, France
Master : Vincent Loechner, Embedded Systems, 32h, M2, Strasbourg University, France

9.2.2. Supervision

PhD in progress : Aravind Sukumaran-Rajam, Enlarging the scope of polyhedral speculative parallelization, November 2012, Philippe Clauss and Alain Ketterlin

PhD in progress : Juan Manuel Martinez Caamaño, Dynamic and flexible generation of parallel loops using a dedicated intermediate representation, November 2013, Philippe Clauss and Philippe Helluy (IRMA lab., University of Strasbourg)

PhD in progress : Jean-François Dollinger, Heterogeneous speculative parallelization, September 2010, Vincent Loechner and Philippe Clauss

PhD in progress : Imen Fassi, Multifor for Multicore, June 2013, Philippe Clauss and Yosr Slama (University El Manar, Tunisia)

PhD in progress : Nabil Hallou, Dynamic binary optimizations, January 2013, Erven Rohou (ALF team) and Philippe Clauss

PhD in progress : Lénaïc Bagnères, Automatic parallelization and optimization for manycore architectures, November 2012, Christine Eisenbeis and Cédric Bastoul

PhD in progress : Alexander Zinenko, Interactive program manipulation, September 2013, Stéphane Huot and Cédric Bastoul

9.2.3. Juries

Philippe Clauss participated to the following HDR jury in 2013:

Date	Candidate	Place	Role
Oct. 11	Fabien Coelho	École des Mines de Paris	Reviewer

Philippe Clauss participated to the following PhD jurys in 2013:

Date	Candidate	Place	Role
Oct. 17	Alexandre Carbon	Univ. Pierre et Marie Curie, Paris	Reviewer
June 28	Antoine Morvan	ENS Cachan	Reviewer
June 12	Damien Hedde	Institut polytechnique de Grenoble	Examiner

Cédric Bastoul participated to the following HDR jury in 2013:

Date	Candidate	Place	Role
Oct. 11	Fabien Coelho	École des Mines de Paris	Examiner

Cédric Bastoul participated to the following PhD jurys in 2013:

Date	Candidate	Place	Role
March 13	Ramakrishna Upadrasta	Paris-Sud University	Examiner
November 27	Dounia Khaldi	École des Mines de Paris	President

Alain Ketterlin participated to the following PhD jury in 2013:

Date	Candidate	Place	Role
Dec. 3	Nathanaël Premilieu	Université de Rennes 1	Examiner

9.3. Popularization

- Cédric Bastoul participated to the *Rencontres Inria-Industrie* in June 2013
- Cédric Bastoul participated to *Fête de la Science* at University of Paris-Sud in October 2013

COMPSYS Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Program Committees, Editorial Boards, and Reviewing Activities

- Christophe Alias was a member of the steering committee of IMPACT 2013 (International Workshop on Polyhedral Compilation Techniques, Berlin, Germany).
- Christophe Alias, Alain Darte, and Paul Feautrier were members of the program committees of IMPACT 2013 and IMPACT 2014 (Vienna, Austria).
- Christophe Alias was member of the program committee of ODES 2013 (i.e., ODES-10, 10th Workshop on Optimizations for DSP and Embedded Systems, Shenzen, China).
- Fabrice Rastello was member of the program committees of CGO 2014 (International Symposium on Code Generation and Optimization, Orlando, Florida) and CRI 2013 (Conférence de Recherche en Informatique, Yaoundé, Cameroun).
- Alain Darte was member of the program committees of DATE 2013 (Design, Automation, and Test in Europe, Grenoble, France) and DATE 2014 (Dresden, Germany), IPDPS 2013 (International Parallel and Distributed Processing Symposium, Boston, Massachusetts) and IPDPS 2014 (Phoenix, Arizona).
- Alain Darte was member of the editorial board of IEEE TECS (Transactions on Embedded Computing Systems) until end of 2013.
- Christophe Alias was a reviewer for the journals JPDC (Journal of Parallel and Distributed Computing), MICPRO (Microprocessors and Microsystems), PPL (Parallel Processing Letters), ACM TRETS (Transactions on Reconfigurable Technology and Systems), TSI (Technique et Science Informatique), CDT (IET Computers and Digital Techniques), IPL (Information Processing Letters).
- Paul Feautrier was a reviewer for ACM TECS, IJPP, IEEE TPDS, ACM TOPLAS, DATE14, IMPACT 2014.
- Alain Darte was a reviewer for DATE'14, IPDPS'14, IMPACT'14, Parallel Computing, ACM TACO, and ACM TECS.
- Laure Gonnord was a reviewer for MSR'13, DAC'13 and AMT'13.

9.1.2. Thematic Quarter on Compilation

Compsys is part of the Labex MILYON, which regroups Institut Camille Jordan, and the mathematics and computer science labs of ENS-Lyon. One of its goal is "to strengthen our international relationships, in particular by organizing thematic quarters which will allow world experts of a subject to gather in Lyon and work together in a stimulating environment." In this context, Alain Darte, helped by Alexandre Isoard and Laetitia Lecot, organized, from April to July 2013, a thematic quarter on compilation techniques (http://labexcompilation.ens-lyon.fr), with a special focus on the interactions with languages and architectures for high performance computing. This thematic quarter (with a total budget of 100 Keuros), consisted, in addition to the "french compilation days" organized separately in Annecy by Laure Gonnord and Fabrice Rastello (April 4-7, 2013), in three international scientific events organized in Lyon or the vicinity.

- A **spring school on polyhedral code analysis and optimizations** (http://labexcompilation.ens-lyon.fr/polyhedral-school), May 13-17, 2013, in Domaine des Hautannes in St Germain au Mont d'Or, the first international school on the polyhedral model and related optimizations. The school covered scheduling theory, algorithms and modeling with integer sets and relations, abstract interpretation, compilation for distributed platforms, array region analysis, vectorization and SIMD optimizations,

through courses given by S. Rajopadhye (Colorado State Univ.), P. Feautrier (Compsys, ENS-Lyon), L.-N. Pouchet (UCLA), S. Verdoolaege (ENS Paris), A. Miné (ENS Paris), U. Bondhugula (IIS Bangalore), A. Darte (Compsys, CNRS), B. Creusillet (Silkan), P. Sadayappan (Ohio State Univ.), N. Vasilache (Reservoir Labs, New York). The school attracted 56 participants, half from France, but also from Germany, the USA, England, Belgium, Spain, China, India, Ireland, and Italy and, interestingly, also from groups that are not familiar with polyhedral optimizations. Roughly half of the participants were PhD students.

- A **dive in languages for high-performance computing** (http://labexcompilation.ens-lyon.fr/hpc-languages), June 29-July 2, 2013 in Résidence Villemanzy in Lyon, organized as a set of long keynotes on CAF (Coarray Fortran), UPC (Unified Parallel C), X10, Chapel, OpenACC & OpenHMPP, Liquid Metal, OmpSs, OpenStream, and some DSL approaches. The keynotes were given by a panel of international experts on compilation for high-performance computing: J. Mellor-Crummey and V. Sarkar (Rice), K. Yelick (Berkeley), R. Schreiber (HP Labs), B. Chamberlain (Cray), D. Grove and R. Rabbah (IBM Watson), A. Cohen (Inria, ENS Paris), R. Badia (UPC Barcelona), F. Bodin (Univ. Rennes, previously Caps Entreprise), Y. Orlarey (Grame), K. Knobe (Intel, Massachusets), P. Sadayappan (Ohio State Univ.). This event regrouped 71 participants, including speakers, and, as we hoped, also attracted people from industry, and not only computer industry.
- **CPC'13, the 17th international workshop on compilers for parallel computing** (http://labexcompilation.ens-lyon.fr/cpc2013), July 3-5, 2013, in Musée Gadagne, in (old) Lyon, a venue that is held every 18 months in Europe since 1989 and that encompasses all areas of parallelism and optimization linked to compilers. The program consisted in 29 talks, from the international community on compilers for HPC (from Japan & Taiwan to the USA, and of course Europe), with 47 participants.

During this compilation thematic quarter, Paul Feautrier and Alain Darte gave the following talks:

- "Array Dataflow Analysis for Polyhedral X10 Programs" (Paul Feautrier) and "Modèles et algorithmes: comprendre de quoi on parle" (Alain Darte) at the French Compiler Community meeting (April 2-4, 2013),
- "The Care and Feeding of Polyhedra" (Paul Feautrier) and "Array Contraction with Lattice-Based Memory Allocation" (Alain Darte) at the Spring School on Polyhedral Code Analysis and Optimizations (May 13-17, 2013),
- "Determinacy Analysis of Polyhedral X10 Programs" (Paul Feautrier), paper with Alain Ketterlin and Eric Violard, at the CPC Workshop (July 3-5, 2013),

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

- Laure Gonnord, Algorithmique et programmation C (60h), L3, Université de Lille 1, Polytech'Lille.
- Laure Gonnord, Architecture des ordinateurs (25h), L3, Université de Lille 1, Polytech'Lille.
- Laure Gonnord, Algorithmique et programmation fonctionnelle et récursive (42h), L1, Université Lyon 1 Claude Bernard.
- Guillaume Iooss, LIF3: algorithmique et programmation fonctionnelle et récursive (28h), L1, Université Lyon 1 Claude Bernard.
- Guillaume Iooss, Programmation 1 (12h), L3, ENS-Lyon.
- Christophe Alias, Architecture des ordinateurs (21h TP), Université Lyon 1.

- Christophe Alias, Compilation (6h CM, 6h TP), ENSI Bourges.
- Christophe Alias, Correction de copies, concours E3A, épreuve informatique MPSI.
- Alexandre Isoard, LIF12: Système et Réseau (32h TP), L3, Université Lyon 1 Claude Bernard.

Master:

- Laure Gonnord, Compilation (24h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord, Introduction aux systèmes et réseaux (52h), M2 Pro, Université Lyon 1.
- Christophe Alias, Compilation (24h CM), M1, ENS-Lyon.
- Christophe Alias, Compilation avancée (8h CM), M2, ENS-Lyon.
- Fabrice Rastello, Compilation avancée (6h CM), M2, ENS-Lyon.
- Fabrice Rastello, SSA-based compiler design (2 days), CRI Cameroun.
- Alexandre Isoard, Compilation (24h TP), M1, ENS-Lyon.
- Guillaume Iooss, Image (24h TP), M1, ENS-Lyon.
- Laure Gonnord also organized, for the Computer Science Department of ENS Lyon, a *research school* for Master students, on synchronous programming. The program can be found at the url: http://laure.gonnord.org/pro/research/sync_research_school.html.

9.2.2. Supervision

- PhD in progress: Guillaume Iooss, "Semantic Tiling", started on September 2011, advisors: Christophe Alias and Sanjay Rajopadhye (Associate Professor, Colorado State University).
- PhD in progress: François Gindraud, started on January 2013, advisors Fabrice Rastello, Albert Cohen (Parkas Inria team)
- PhD in progress: Duco Van Amstel, started on January 2013, advisors Fabrice Rastello, Benoit Dupont-de-Dinechin (Kalray)
- PhD in progress: Diogo Nunes Sampaio, started on October 2013, advisor Fabrice Rastello
- PhD in progress: Alexandre Isoard, started in September 2012, advisor Alain Darte

9.2.3. Juries

- Laure Gonnord participated to the Jury of Clement Guy's PhD defense (in Rennes) entitled "Facilités de typage pour l'ingénierie des Langages". This PhD was supervised by J.M. Jézéquiel (Professor, Rennes University), and B. Combemale (Assistant Professor, Rennes University) and S. Derrien (Professor, Rennes university).
- Christophe Alias participated to the Jury of Antoine Morvan's PhD defense (in Rennes) entitled "Utilisation du modèle polyédrique pour la synthèse d'architectures pipelinées". This PhD thesis was supervised by S. Derrien (Professor, Rennes University), and P. Quinton (Professor, Rennes University).
- Fabrice Rastello participated to the jury of Alexandre Carbon's PhD defense, entitled "Accélération matérielle de la compilation à la volée pour les systèmes embarqués".
- Paul Feautrier was a reviewer for the HDR of Stephane Mancini (Grenoble) and for the PhD of Amira Mensi (Paris).
- Alain Darte was a reviewer for the PhD thesis of Cupertino Miranda (Paris 11), entitled "Erbium: Reconciling languages, runtimes, compilation and optimizations for streaming applications" and supervised by Albert Cohen (DR Inria, Parkas team).

CONTRAINTES Project-Team

9. Dissemination

9.1. Scientific Animation

- Grégory Batt's invited seminars:
  - Long-term model predictive control of gene expression, in *Bison seminar*, ETHZ, Zurich, March 2013
  - Modeling intrinsic and extrinsic variability: models, model identification methods and noise conversion, *Haredhol seminar*, ENS Paris, Paris, April 2013
  - Comprendre et contrôler le fonctionnement des cellules: apport de la biologie computationnelle, Seminar *Groupement de recherche interdisciplinaire sur les systèmes biologiques (Grisbi)*, Montpellier, Oct 2013
  - Comprendre et contrôler le fonctionnement des cellules: apport de la biologie computationnelle, *Symposium franco-britannique sur la biologie de synthèse*, London, Oct 2013
  - Cells driven by computers. *Pharmacometry and Bioinformatics Day*, Sanofi, Paris, Dec 2013

  He has been a member of the EraSynBio evaluation committee (Lisbon), judge at iGEM competition (Lyon), and animator of the axis "Modélisation des réseaux biologiques, biologie systémique et synthétique" of the Groupement de Recherche "Bioinformatique moléculaire" (GdR BIM). He was member of the PhD advisory committees of Adrien Henry (laboratoire de génétique végétale du Moulon, Orsay) and of Géraldine Célière (Bang group, Inria Paris-Rocquencourt). He was a reviewer for Integrative Biology, PLoS Computational Biology, ACS Synthetic Biology, European Conference on Control, and Computational Methods in Systems Biology conference
- Xavier Duportet's invited seminar and contributed poster presentations:
  - Keystone Symposia on Precision Genome Engineering and Synthetic Biology, Colorado, USA, March 17-22
  - Synthetic Biology conference (SB6.0), London, July 9-12

  He has been involved in technological transfer activities:
  - Provisional patent application: High-throughput discovery of recombinase sites towards the engineering of recombinase specificity
  - Consulting on mammalian synthetic circuit design for Lung LLC, USA

  Xavier is also the President of a non-profit organization to promote science and technology entrepreneurship among European students and scientists and organizing the Hello Tomorrow Challenge, a European startup competition.
- François Fages is a member of
  - Editorial Board of RAIRO Operations Research,
  - Steering Committee of the International Conference series on Computational Methods in Systems Biology (CMSB).
  - Scientific Advisory Board of the Doctorate School Frontières du Vivant of the University Paris Descartes
  - "Comité de pilotage" of the OSEO BioIntelligence project, coordinated by Dassault-Systèmes
  - "Comité scientifique du LIFO", University of Orléans

– "Commission de spécialistes", University of Lille.

He was member of the program committees of CHR'13 (Tenth International Workshop on Constraint Handling Rules Berlin, Germany – July 13th, 2013), CMSB'13 (Eleventh Conference on Computational Methods in Systems Biology, IST Klosterneuburg, Austria, September 2013), FroCoS'13 (Frontiers of Combining Systems, co-located with Tableaux 2013, Nancy, France, September 18-20, 2013), HSB'13 (Second International Workshop on Hybrid Systems and Biology associated to ECAL 2013, Taormina, Italy, September 2, 2013), ICLP'13 (29th International Conference on Logic Programming 24 - 29 August 2013, Istanbul, Turkey), WCB'13 (Workshop on Constraint-Based-Methods for Bioinformatics, Budapest, Hungary, co-located with CP'13, Uppsala, Sweden September 16-20, 2013), ICORES'13 (second International Conference on Operations Research and Enterprise Systems, held in conjunction with h ICAART 2013 and ICPRAM 2013, Barcelona, Spain, Feb 2013).

He has reviewed articles for the following journals: ACM Transactions on Computational Logics, Artificial Intelligence, Journal of Logic and Computation, PLOS Computational Biology, Annals of Operations Research, Information and Computation, Journal of Mathematical Biology, Constraints, BMC Systems Biology,

François Fages was reviewer of research grants for

– the Netherlands Organisation for Scientific Research (NWO),
– the Research Foundation Flanders (FWO)

Invited talks:

– BRICS-CCI, 1st BRICS Countries Conference on Computational Intelligence, Recife, Brazil, October 2013.
– Symposium Biointelligence, Sophia-Antipolis, July 2013.
– Interdisciplinary Symposium on Signals and Systems for Medical Applications, Paris, 3-4 Jun 2013.

- Thierry Martinez was member of the Program Committee of CHR'13. He acted as reviewer for the journal Constraints, and for the conferences Concur'13, FROCOS'13 and ICLP'13.
- Sylvain Soliman acted as reviewer for LICS'13, and CMSB'13, and as member of the Program Committees of WLPE'13, JFPC'13 and SASB'13. He was also reviewer for the Austrian Science Fund (FWF) stand alone project proposals.
- Denis Thieffry is currently
  – member of the INSERM CSS2 evaluation/recruitment commission;
  – member of the board of the PhD Program Complexity in Post-Genomic Biology of the University of Torino;
  – member of the program committees for ISMB, JOBIM, CMSB, and SASB;
  – Editor of BioSystems;
  – Associated Editor of PLoS Computational Biology; as well as of BMC Systems Biology;
  – Adviser for the PLoS Biology Education series.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Contraintes is affiliated to the Doctoral school of Mathematical Science of the University Paris Diderot, and to the interdiciplinary Doctoral school "Frontières du Vivant" of the University Paris Descartes.

The following courses have been given by members of Contraintes:

Ecole thématique CNRS “Biologie des Réseaux”, Ile de Porqueroles, François Fages (6h), Denis Thieffry (4h).

Master M2 course C2-19 on *Computational Methods for Systemic and Synthetic Biology*, Master Parisien de Recherche en Informatique (MPRI) François Fages (responsible, 12h), Grégory Batt (12h), Denis Thieffry (12h).

Interdisciplinary Master in Life Science at the Ecole Normale Supe´rieure, Paris. Denis Thieffry (coordinator).

Master M2 course C2-35-1 on *Constraint Programming*, Master Parisien de Recherche en Informatique (MPRI) Sylvain Soliman (responsible, 24h) [beginning of the 2013-2014 academic year].

Master M1 course on *Computational Biology*, Master Approches Interdisciplinaires du Vivant (AIV), Grégory Batt (coordinator, 48h).

Master M2 course *Dynamical Modelling of Cellular Regulatory Networks*, Master of Biology of Cellular Systems, Grégory Batt (6h).

9.2.2. Supervision

PhD : Faten Nabli, “Approches de programmation par contraintes pour l’analyse des propriétés structurelles des réseaux de Petri et application aux réseaux biochimiques”, Université Paris Diderot, Paris, 10/07/2013, Dir. François Fages and Sylvain Soliman

PhD : Jannis Uhlendorf, “Real-time feedback control of gene expression”, Paris Diderot University, Paris, 19/04/2013, Dir. Grégory Batt and Pascal Hersen (MSC)

PhD in progress : François Bertaux, Université Pierre et Marie Curie, Paris, Sept 2011, Dir. Dirk Drasdo (EPI BANG) and Grégory Batt

PhD in progress : Xavier Duportet, Université Paris Descartes, Paris, Oct 2010, Dir. Grégory Batt, François Fages and Ron Weiss (MIT)

PhD in progress : Steven Gay, Université Paris Diderot, Paris, Oct 2009, Dir. François Fages and Sylvain Soliman,

PhD in progress : David Fournier, Université Paris Diderot, Paris, Oct 2011, Dir. François Fages and Denis Mulard (General Electric),

PhD in progress : Jean-Baptiste Lugagne, Université Paris Diderot, Paris, Oct 2012, Dir. Grégory Batt, François Fages and Pascal Hersen (MSC)

PhD in progress : Artemis Llamosi, Université Paris Diderot, Paris, Nov 2012, Dir. Grégory Batt, Jean-Marc di Meglio and Pascal Hersen (MSC)

PhD in progress : Pauline Traynard, Université Paris Diderot, Paris, Oct 2012, Dir. François Fages and Denis Thieffry (ENS)

PhD in progress : Luma Vittorino, Université Paris Diderot, Paris, Oct 2012, Dir. François Fages,

9.2.3. Juries

HDR of Cédric Lhoussaine, University of Lille. Dec 2013. Reviewer François Fages.

HDR of Nicolas Le Novère, University of Bordeaux. Nov 2013. Reviewer François Fages and Denis Thieffry.

PhD Thesis defense of Geoffrey Andrieux. University of Rennes. Jul 2013. François Fages.

PhD Thesis defense of Sucheendra Palaniappan, NUS, Singapore. June 2013. Reviewer Grégory Batt.

PhD Thesis defense of Andreas Milias-Argeitis, ETHZ. March 2013. Reviewer Grégory Batt.

MSc Thesis defenses of Lakshmeesh Maruthi and Yifan Pan, TU Delft. September 2013. Grégory Batt.

DREAMPAL Team

9. Dissemination

9.1. Scientific Animation

F. Guyomarch is a member of the ComPAS program committee. Jean-luc Dekeyser is PC Member of DSD, Reconfig, Recosoc and Sympa.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : F. Guyomarch, Algorithmique et programmation, 144h, L1, IUT-A (Université de Lille 1), France

Licence : F. Guyomarch, Modélisation et théorie des langages, 64h, L2, IUT-A (Université de Lille 1), France

Licence : Philippe Marquet, Introduction to Computer Science, 15h, Secondary Education Teatcher Training, Université Lille 1, France

Licence : Philippe Marquet, System Programming, 60h, L3, Université Lille 1, France

Master: Philippe Marquet, Design of Operating System, 60h, M1, Université Lille 1, France

Master: Philippe Marquet, Web of Things: Embedded System Programming, 20h, M1, Université Lille 1, France

Master: Philippe Marquet, Parallel and Distributed Programming, 24h, M1, Université Lille 1, France

Master: Philippe Marquet, Introduction to Innovation and Research, 15h, M2, Université Lille 1, France

Licence : Jean-Luc Dekeyser, Architecture élémentaire, 85h, L2, Université Lille 1, France

Master: Jean-Luc Dekeyser, Architecture évoluée, 90h, M1, Université Lille 1, France

Licence : Rabie Ben Atitallah, Introduction to Computer Architecture and Operating System, 36h, L2, Université de Valenciennes et du Hainaut-Cambrésis, France

Licence : Rabie Ben Atitallah, Algorithms and Language C Programming, 48h, L2, Université de Valenciennes et du Hainaut-Cambrésis, France

Master: Rabie Ben Atitallah, Tools for Embedded System Design, 32h, M2, Université de Valenciennes et du Hainaut-Cambrésis, France

Master: Rabie Ben Atitallah, Development and Compilation of Embedded Application, 32h, M2, Université de Valenciennes et du Hainaut-Cambrésis, France

Master: Vlad Rusu, Software Specification and Verification, 27 h, Univ. Lille 1, France

Master: Vlad Rusu, Advanced Software Architecture, 42 h, Univ. Lille 1, France.

9.2.2. Committees

Vlad Rusu participated as a reviewer in the PhD committees of Rouwaida Ben-Abdallah (Univ. Rennes) and Pierre-Nicolas Tolitte (Conservatoire National des Arts et Métiers, Paris).

9.3. Popularization

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

Philippe Marquet is involved in scientific popularization, mostly within the context of a partnership of between the Inria Lille - Nord Europe Research Center, the University Lille 1, and the Académie of Lille. 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. This year, 30 “proviseurs”, 30 teachers, and about 170 students spend half a day on the Plateau. He has designed the isnlilleacademie.fr web site (http://www.isnlilleacademie.fr), an information site on the *spécialité ISN* (computer and digital science in french high schools) for pupils, students, and their parents’.

Philippe Marquet is a member of the editorial board of 1024, the new 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.

INDES Project-Team

8. Dissemination

8.1. Seminars and conferences

- **Pejman Attar** gave a talk about security in concurrency at Paris 7 in february 2013. He participated March in *rencontres du numérique de l'ANR* and presented a poster about his work and the PARTOUT ANR team work.
- **Nataliia Bielova** was invited to present her work on web security in Labex Security day.
- **Ilaria Castellani** participated in March in the 1st working group (WG) meeting of the BETTY Action, in Rome, where she animated the discussion of the Security WG. In September, she took part in the 2nd WG meeting of BETTY, in Madrid, where she again animated the discussion of the Security WG. In August 2013, Ilaria Castellani participated in the workshop "25 Years of Combining Compositionality and Concurrency" (WS25CCC), in Königswinter, Germany, and in the 8th International Symposium on Trustworthy Global Computing (TGC 2013), in Buenos Aires, Argentina. In both of them, she presented her joint work with Pejman Attar [11]. In Buenos Aires, she also took part in the annual meeting of the IFIP WG 1.8 on Concurrency Theory.
- **Cyprien Nicolas** gave a talk about "Cable-Driven Robots with Wireless Control Capability for Pedagogical Illustration of Science" at the 8th National Conference of "Control Architecture of Robots" in Angers, France, June, 12th 2013 [13].
- **Tamara Rezk** was invited to present her work on web security in IRISA Rennes in January and in University of Cordoba in March. She gave a talk in the Labex Security day.
- **Manuel Serrano** gave a seminar about Web programming in the seminar series associated with the course of Gérard Berry at Collège de France called *Informatique du Temps et des Évenements*. He participated in a one-week seminar in Brussels on Secure Cloud and Reactive Internet Programming Technology, where he gave a talk on HipHop. He presented the results of the PWD projet at the ANR *Rencontres du numérique* in Paris. Manuel Serrano gave a lecture on Hop at the ECOOP Programming Summer School.

8.2. Animation

- **Ilaria Castellani** is a member of the editorial board of *Technique et Science Informatiques*. She is a member of the IFIP WG 1.8 on Concurrency Theory. She is a member of the Management Committee of the BETTY Action, and the chair of the BETTY working group on Security. She was a member of the programme committee of the workshop EXPRESS/SOS 2013.
- **Tamara Rezk** was a member of the programme committees of JAIIO'13, CIBSI'13, TGC'13, LATIN'14, TIBETS'13, SOFSEM'14. She was invited to be in the PC of CSF'14. She was invited by the Estonian Research Council as an external expert to the evaluation of a research project. She is part of the organizing committee for the Labex Security day with **Nataliia Bielova**.
- **Manuel Serrano** is a member of the editorial board of the *Journal of Functional Languages*. He is the coordinator of the ANR DEFIS project PWD. He served on the program committee of the *16th Practical Aspects of Declarative Languages* (PADL'14) conference. He was a referee for the *Lisp in Summer Projects*. He was the co-program chair of the *European Lisp Symposium* (ELS'13).

8.3. Teaching - Supervision - Juries

8.3.1. Teaching

DUT: **Cyprien Nicolas**, *Introduction aux systèmes informatiques*, 36ETD, S1, IUT Nice Côte d'Azur, UNS, France. *Architecture Systèmes et Réseaux*, 16ETD, S3, IUT Nice Côte d'Azur, UNS, France.

Licence: **Cyprien Nicolas**, *Algorithmique et Complexité*, 30ETD, Licence Professionnelle SIL, IUT Nice Côte d'Azur, UNS. **Yoann Couillec**, *Algorithmique - Programmation objet - Python*, 36 ETD, L2, University of Nice Sophia Antipolis. **Vincent Prunet**, *Algorithms and Data Structures*, 80 ETD, L2, Lycée International de Valbonne, (Inria action to promote early CS courses in all scientific curricula).

Master: **Ilaria Castellani**, *Programmation et sécurité des applications du web*, 13.5 ETD, M2, University of Nice Sophia Antipolis. **Tamara Rezk**, *Programmation et sécurité des applications du web*, M2, University of Nice. *Programming the Diffuse Web*, 13.5 ETD, M2, University Paris 6 (UPMC), France. *Provable cryptography* 28h ETD, M2 University of Nice Sophia Antipolis. **Manuel Serrano**, *Programming the Diffuse Web*, 13.5 ETD, M2, University Paris 6 (UPMC), France.

PhD: **Manuel Serrano** gave a full-day seminar on Hop at the *École des Jeunes Chercheurs en Programmation* (Rennes).

8.3.2. Supervision

PhD: **Pejman Attar**, *Towards a safe and secure synchronous language*, University of Nice, 1/10/2010, **Frédéric Boussinot** and **Ilaria Castellani**.

PhD in progress: **Cyprien Nicolas**, *Orchestrating multi-tier programming languages*, University of Nice, 1/09/2010, **Gérard Berry** and **Manuel Serrano**.

PhD in progress: **Johan Grande**, *Conception et implantation d'un langage de programmation concurrente modulaire*, University of Nice, 1/10/2010, **Gérard Boudol** and **Manuel Serrano**.

PhD in progress: **Yoann Couillec**, *Langages de programmation et données ouvertes*, University of Nice, 1/10/2012, **Manuel Serrano** and **Patrick Valduriez**.

PhD in progress: **José Santos**, *Language based approach for information flow analysis in distributed mobile code*, University of Nice, 1/12/2010, **Tamara Rezk**.

Master internship: **Jérôme Brunel** master thesis at University of Nice-Sophia Antipolis, tutored by **Tamara Rezk**. **Gerard Boudol** has supervised the intership (Master Recherche) of Arthur Guillon, on relaxed memory models. The long term objective was to investigate the quantitative aspects of such models, but a first phase of the study consisted in refining an abstract model previously introduced by Boudol, Petri and Serpette. More precisely, this model was refined so as to provide an adequate semantics for PowerPC memory barriers, a notoriously difficult topic. To this end we extended the notion of visibility, attached to memory write operations, to these barriers. In this way, we achieved an accurate semantics of these synchronization operations with respect to the series of tests on PowerPC machines developed by Luc Maranget. In a second phase, some requirements for a notion of probabilistic memory model were identified.

8.3.3. Juries

Ilaria Castellani was a member of the jury of the PhD thesis of Fabrizio Montesi, IT University of Copenhagen.

8.4. Popularization

The Web is becoming the richest platform on which to create computer applications. Its power comes from three elements: modern Web browsers enable highly sophisticated graphical user interfaces (GUIs) with 3D, multimedia, fancy typesetting, among others; calling existing services through Web APIs makes it possible to develop sophisticated applications from independently available components; and open-data availability allows access to a wide set of information that was unreachable or that simply did not exist before. The combination of these three elements has already given birth to revolutionary applications such as GoogleMaps, radio podcasts, and social networks.

The next step is likely to be incorporating the physical environment into the Web. Recent electronic devices are equipped with various sensors (GPS, cameras, microphones, metal detectors, speech commands, thermometers, motion detection, and so on) and communication means (IP stack, telephony, SMS, Bluetooth), which enable applications to interact with the real world. Web browsers integrate these features one after the other, making the Web runtime environment richer every day. The future is appealing, but one difficulty remains: current programming methods and languages are not ideally suited for implementing rich Web applications. This is not surprising as most have been invented in the 20th century, before the Web became what it is now.

Traditional programming languages have trouble dealing with the asymmetric client-server architecture of Web applications. Ensuring the semantic coherence of distributed client-server execution is challenging, and traditional languages have no transparent support for physical distribution. Thus, programmers need to master a complex gymnastics for handling distributed applications, most often using different languages for clients and servers. JavaScript is the dominant Web language but was conceived as a browser only client language. Servers are usually programmed with quite different languages such as Java, PHP, Ruby, etc. Recent experiments such as Node.js propose using JavaScript on the server, which makes the development more coherent; however, harmonious composition of independent components is still not ensured.

In 2006, three different projects, namely, GWT from Google, Links from the University of Edinburgh, and HOP from Inria (`http://www.inria.fr`) [6], offered alternative methods for programming Web applications. They all proposed that a Web application should be programmed as a single code for the server and client, written in a single unified language. This principle is known as multitier programming.

Links is an experimental languages in which the server holds no state and functions can be symmetrically called from both sides, allowing them to be declared on either the server or the client. These features are definitely interesting for exploring new programming ideas, but they are difficult to implement efficiently, making the platform difficult to use for realistic applications.

GWT is more pragmatic. It maps traditional Java programming into the Web. A GWT program looks like a traditional Java/Swing program compiled to Java bytecode for the server side and to JavaScript for the client side. Java cannot be considered as the unique language of GWT, however. Calling external APIs relies on JavasCript inclusion in Java extensions. GUIs are based on static components declared in external HTML files and on dynamic parts generated by the client-side execution. Thus, at least Java, Javascript, and HTML are directly involved.

The HOP language takes another path relying on a different idea: incorporating all the required Web-related features into a single language with a single homogeneous development and execution platform, thus uniformly covering all the aspects of a Web application: client-side, server-side, communication, and access to third-party resources. HOP embodies and generalizes both HTML and JavaScript functionalities in a Scheme-based platform that also provides the user with a fully general algorithmic language. Web services and APIs can be used as easily as standard library functions, whether on the server side or client side.

In order to popularize HOP, we have written a paper for targeting engineers which presents on overview of the HOP language and its development environment. It has been simultaneously published in ACM Queue and Communications of the ACM [5]. We have also given several demonstrations of the system. In particular, Cyprien Nicolas has co-developed application software for an educational cable robot (Coprin) presented at the Fête de la Science, in November. The demo consisted in a Cable bot built by a Coprin student and piloted by Hop, the software being written by a Indes student. The demo took place in front of four classes of High School students.

8.5. Transfer

8.5.1. Diffuse Robotics

Dissemination of the HOP technology has become a priority for the team now that HOP is actually used to develop large projects. In 2012, a further step was taken with the allocation of dedicated resources missioned to develop and transfer the application portfolio to the industry. The team has focused on bringing web awareness

to personal assistance robots developed by the Coprin team, also at Inria CRISAM, in line with one of the top strategic orientations of Inria. Using web protocols as a native framework greatly simplifies the integration of the robot as a web entity, and the use of remote web services to manage, monitor or extend the features of the robot. The behavior of a HOP robot is specified in HOP and orchestrated within diffuse HOP run time agents embedded within the robot elements, in charge of handling communication and control between platforms and with remote web services. The project, code-named *Diffuse Robotics*, builds on the experience gained in using HOP for home automation over the recent years, adding in 2012 the support of versatile robotic computing platforms and associated mechanics and sensor hardware and a state of the art plug and play framework for automatic device and service discovery. Among the direct benefits of relying on a web framework are the ability to use any web enabled device such as a smartphone or tablet to drive the robot. Also, it is much simpler to put in place remote diagnostic and monitoring services by leveraging on existing robot sensors and the HOP framework.

PAREO Project-Team

8. Dissemination

8.1. Scientific Animation

Jean-Christophe Bach:

- Member of the LORIA laboratory council
- Member of the organizing committee of the “Journées GDR–GPL” colocated with the AFADL and CIEL conferences

Christophe Calvès

- Member of the organizing committee of the “Journées GDR–GPL” colocated with the AFADL and CIEL conferences

Horatiu Cirstea:

- PC member of RuleML 2013 (International RuleML Symposium on Rule Interchange and Applications).
- PC member of SCSS 2013 (International Symposium on Symbolic Computation in Software Science).
- Steering committee of RULE.
- Responsible for the Master speciality “Logiciels: Théorie, méthodes et ingénierie”.
- Member of the organizing committee of the “Journées GDR–GPL” colocated with the AFADL and CIEL conferences

Sergueï Lenglet:

- Member of the organizing committee of the “Journées GDR–GPL” colocated with the AFADL and CIEL conferences
- Invited speaker at the “Journées LAC”
- Reviewer for the TCS (Theoretical Computer Science) journal

Pierre-Etienne Moreau:

- Member of the GDR–GPL (CNRS Research Group on Software Engineering) board.
- Member of the national committee for Inria “Médiation Scientifique”.
- Head of the local committee for Inria “détachements” and “délégations”.
- Head of the Computer Science department at Ecole des Mines de Nancy.
- President of the organizing committee of the “Journées GDR–GPL 2013” colocated with the AFADL and CIEL conferences
- PC member of SLE 2013 (6th International Conference on Software Language Engineering), SCSS 2013 (5th International Symposium on Symbolic Computation in Software Science),
- Member of the organizing committee of WASDeTT 2013 (4th International Workshop on Academic Software Development Tools and Techniques)

Sorin Stratulat:

- Member of the LITA Laboratory Council.
- Member of the program committee of the 9th International Conference on Information Assurance and Security (IAS '13)
- Member of the program committee of the 6th International Conference on Computational Intelligence in Security for Information Systems (CISIS'13)
- Member of the program committee of the 5th International Symposium of Symbolic Computation in Software Science (SCSS '13)
- Tutorial speaker at the Conference on Automated Reasoning with Analytic Tableaux and Related Methods (TABLEAUX 2013)
- Speaker at
  - Workshop on Inductive Theorem Proving 23-24 November 2013, Imperial College London, UK
  - LIX Colloquium on the Theory and Application of Formal Proofs, 5-7 November 2013, Ecole Polytechnique, Palaiseau, France
  - Workshop on Proof Search in Axiomatic Theories and Type Theories (PSATTT), 8 November 2013, Ecole Polytechnique, Palaiseau, France

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Pierre-Etienne Moreau, Responsible of the course "Introduction to Algorithms and Programming" (http://www.depinfonancy.net/s5/tcs13), first year at Mines-Nancy (150 students), Université de Lorraine, France

8.2.2. Supervision

PhD in progress : Jean-Christophe BACH, "Transformation de modèles et certification", November 1st 2010, Pierre-Etienne Moreau

PhD in progress : Amira HENAIEN, "Certification du raisonnement formel porté sur des systèmes d'information critiques.", November 1st 2010, Sorin Stratulat

8.2.3. Juries

Horatiu Cirstea:

PhD committee of Henri Debrat, "Certification formelle de la correction d'algorithmes de Consensus", Nancy 2013

Pierre-Etienne Moreau:

PhD committee of Mathieu Giorgino, reviewer, Toulouse, 2013: "Inductive Representation, Proofs and Refinement of Pointer Structures"

PhD committee of Clément Guy, reviewer, Rennes, 2013: "Facilités de typage pour l'ingénierie des langages"

PhD committee of Pengfei Liu, reviewer, Bordeaux, 2013: "Intégration de politiques de sécurité dans des systèmes ubiquitaires"

PhD committee of Laurent Wouters, Paris, 2013: "Multi-Domain Expert-User Modeling Infrastructure"

8.3. Popularization

Participants: Jean-Christophe Bach, Pierre-Etienne Moreau.

Jean-Christophe Bach participated to scientific mediation by proposing several activities to demonstrate the *algorithmic thinking* at the core of the Computer Science without requiring any computer or even electric devices. These activities are the first part of the CSIRL (Computer Science In Real Life) project which aims to popularize computer science and to initiate children, school students and non-scientists into this domain. These activities were presented during the high school students welcome at LORIA and Inria - Nancy Grand Est, and also during APMEP [1] days. Jean-Christophe Bach also took part to the "Fête de la science" in October.

Jean-Christophe Bach was also involved in popularization activities with Interstices [2] by writing short debunking articles ("Idées reçues") for non computer scientists about Church's thesis and Turing's work [15]. Other popularization articles are still under work.

Pierre-Etienne Moreau gave two lectures about "Robotics and Programming" in the ISN course (Informatique et Science du Numérique), in order to help professors of "classes de terminale" to teach this discipline.

Pierre-Etienne Moreau organized a three day course about "Algorithms, Programming and Databases" in order to help professors of "classes préparatoires aux grandes écoles" to teach this discipline.

[1] http://www.apmep.asso.fr/
[2] http://interstices.info

TASC Project-Team

9. Dissemination

9.1. Scientific Animation

- Nicolas Beldiceanu:
  - Head of the Inria TASC team and LINATASC team.
  - Member of the program committee of CP 2013.
  - Member of the program committee of CPAIOR 2013.
  - Member of the program committee of CPAIOR 2014.
  - Member of the program committee of CP 2014.
  - Reviewer for the Constraints Journal.
- Fréderic Benhamou:
  - Vice-President for Research of Nantes University, France.
- Gilles Chabert:
  - Member of the program committee of JFPC 2013.
  - Reviewer for CP 2013.
  - Reviewer for IJCAI 2013.
  - Supervision PhD committee Aymeric Bethencourt (ENSTA Bretagne), Gilles Chabert.
  - Supervision PhD committee of Remy Guyonneau (ISTIA Angers), Gilles Chabert.
- Sophie Demassey:
  - Member of the application track program committee of CP 2013.
- Jean-Guillaume Fages:
  - Member of the program committee of JFPC 2014.
- Narendra Jussien:
  - Head of the computer science department at EMN.
  - Director of the series *Operations Research and Constraint Programming* from ISTE/Wiley.
  - Member of the program committee of CP 2013.
  - Member of the program committee of CPAIOR 2013.
- Xavier Lorca:
  - Member of the program committee of JFPC 2013.
  - Managing the topic *constraints and optimization* within the LINA.
  - Member of the LINA lab council.
  - Reviewer for IJCAI 2013.
  - Reviewer for RAIRO.
  - Reviewer for the Constraints Journal.
- Eric Monfroy:
  - Co-chair of the ACM SAC CSP track 2013.
  - Co-chair of the ACM SAC CSP track 2014.
  - Member of the program committee of CHR 2013.

  - Member of the program committee of JFPC 2013.
  - Reviewer for IEEE TEC.
  - Reviewer for Information Sciences (Elsevier).
  - Co-Editor of the CP Newsletter (until july 2013).
  - Member of the *Conseil d'Administration* of the AFPC.
- Charles Prud'Homme:
  - Member of the program committee of JFPC 2014.
- Florian Richoux:
  - Member of the program committee of Learning and Intelligent OptimizatioN Conference" 2014 (LION 8).
  - Member of the program committee of ACM Symposium On Applied Computing 2014 (SAC'14).
  - Member of the program committee of JFPC 2014.
  - Reviewer for the journal IEEE Transactions on Computational Intelligence and AI in games.
  - Reviewer for the conference CP 2013.
- Thierry Petit:
  - Co head of the LINA TASC team.
  - Member of the program committee of CP 2013.
  - Member of the program committee of CPAIOR 2014.
  - Member of the program committee of ECAI 2014.
  - Program chair of JFPC 2014.
  - Reviewer for the Constraints Journal.
- Charlotte Truchet:
  - Equal Opportunity Officer for Nantes University since October 2012, for gender equality issues.
  - Program chair of JFPC 2013.
  - Member of the program committee of JFPC 2014.
  - Reviewer for IJCAI 2013.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: N. Beldiceanu, Constraint (Master ORO), 30h, M2, Nantes University, France.

Master: N. Beldiceanu, Logic Programming, 32h, M2, Mines de Nantes, France.

Master: N. Beldiceanu, Gipad end project, 8h, M2, Mines de Nantes, France.

Licence: N. Beldiceanu, Imperative Programming, 12h, L3, Mines de Nantes, France.

Licence: N. Beldiceanu, Interface, 12h, L3, Mines de Nantes, France.

Master: G. Chabert, Non-linear programming, 20h, M2, Mines de Nantes, France.

Master: G. Chabert, Non-linear optimization, 20h, M1, Mines de Nantes, France.

Master: G. Chabert, Non-linear optimization, 24h, M1, Nantes University, France.

Licence: G. Chabert, Variational calculus, 12h, L3, Mines de Nantes, France.

Licence: G. Chabert, Numerical methods, 21h, L3, Mines de Nantes, France.

Licence: G. Chabert, Simulation and parameter estimation, 18h, L3, Mines de Nantes, France.

Licence: G. Chabert, Numerical integration, 15h, L3, Mines de Nantes, France.

Licence: G. Chabert, Supervisions of projects, 66h.

Master: X. Lorca, Head of the major of the Master in Engineering, Computer Science for Decision Support, 30h, M2, Mines de Nantes, France.

Master: X. Lorca, Algorithms and Complexity, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Data Warehouse and Data Analysis, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Graph Theory, Algorithms, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Business Intelligence, 20h, M2, Mines de Nantes, France.

Master: X. Lorca, IT System and Software Development, 20h, M2, Mines de Nantes, France.

Master: X. Lorca, Implementation Project, 20h, M2, Mines de Nantes, France.

Licence: E. Monfroy, Algorithm, 40h, L1, Nantes University, France.

Licence: E. Monfroy, Algorithm 2, 16h, L2, Nantes University, France.

Licence: E. Monfroy, Logic, 40h, L2, Nantes University, France.

Licence: E. Monfroy, Language theory, 96h, L3, Nantes University, France.

Master: T. Petit, Director of the Discrete Optimization degree, M2, GIPAD, Mines Nantes, France.

Master: T. Petit, Director of the Artificial Intelligence and Constraint Programming degree, M2, GIPAD, Mines Nantes, France.

Master: T. Petit, Scheduling and optimization, M2, 18h, Mines de Nantes, France.

Master: T. Petit, Constraint Programming in Choco, M2, 20h, Mines de Nantes, France.

Master: T. Petit, Supervisor of two final 6 months projects, M2, 12h, Mines de Nantes, France.

Licence: T. Petit, Data structures, L2, 20h, Mines de Nantes, France.

Licence: T. Petit, SQL, L2, 19h, Mines de Nantes, France.

Licence: T. Petit, HMI, L2, 13h , Mines de Nantes, France.

Licence: T. Petit, Data processing integration in HMI, L2, 10h, Mines de Nantes, France.

Licence: T. Petit, Java, L1, 40h, Mines de Nantes, France.

Licence: T. Petit, IPIPIP project, L1, 5h, Mines de Nantes, France.

Licence: T. Petit, ACDC project, L1, 7.5h, Mines de Nantes, France.

Master: F. Richoux, Constraint Programming, 12h, M2, University of Nantes, France.

Licence: F. Richoux, Design Patterns in Object-Oriented Programming, 86h, L3, University of Nantes, France.

Licence: F. Richoux, Algorithm and Data Structures, 45h, L2, University of Nantes, France.

Licence: F. Richoux, Introduction to Computer Science, 28h, L1, University of Nantes, France.

Licence: Charlotte Truchet, Algorithms and Programming, 46h, L1, University of Nantes, France.

9.2.2. Supervision

PhD: Arnaud Letort, Scalable multi-dimensional resources scheduling constraints [11], Nantes University, October 28 2013, Nicolas Beldiceanu.

Internship of Julie Laniau with Charlotte Truchet on *using constraints for checking audio real time programs* (from February 2013 to June 2013).

PhD in progress: Bruno Belin, Interactive conception of sustainable urban environments with constraints, September 2011, Charlotte Truchet, Marc Christie, Fréderic Benhamou.

PhD in progress: Jean Guillaume Fages, Graph Theory in Constraint Programming, Theory and application to several graph covering problems, October 2011, Xavier Lorca, Nicolas Beldiceanu.

PhD in progress: Charles Prud'Homme, Controlling Propagation and Search within a Constraint Solver, October 2011, Xavier Lorca, Narendra Jussien, Rémi Douence, defense planned for February 2014.

PhD in progress: Alban Derrien, Constraint propagation with limited time complexity, October 2012, Thierry Petit, Nicolas Beldiceanu.

PhD in progress: Ignacio Sala Donoso, Packing curved shapes, May 2013, Gilles Chabert, Nicolas Beldiceanu.

PhD in progress: Alejandro Reyes Amaro, New parallel algorithms for combinatorial optimization, October 2013, Florian Richoux, Eric Monfroy.

9.2.3. Juries

- N. Beldiceanu, Member of the PhD committee of the thesis of Arnaud Letort (Univ. Nantes, October 28, 2013).
- G. Chabert, Member of the PhD committee of the thesis of Remy Guyonneau (ISTIA Angers).

9.3. Popularization

- Within the context of the global constraint catalog:
  - we provide more exercises (up to 55 currently) with their solution and a web version allowing some interaction will be available in spring 2014.
  - the effort for converting and completing the 900 figures of the catalog using TikZ has been continued up to a point where beginning 2014 only 150 figures need still to be converted.
- Within the context of the library IBEX the following courses were given:
  - A workshop in June and December 2013 in Brest (ENSTA).
  - A user oriented course in July 2013 at the doctoral days of the GDR Macs in Strasbourg.
  - A developer oriented course *IBEX days* in October 2013 in Paris (Ecole des Ponts, Paritech).
- A the 2013 edition of the Fête de la Science (Nantes University):
  - Two talks on *Artificial Intelligence and real time strategy games* were given by Florian Richoux.
  - One talk on *Challenges around optimizations problems* was given by Xavier Lorca.
  - One half day discussing and answering questions around the work of professor and researcher in computer science with young persons (17 years old) was spent by Nicolas Beldiceanu.

ESPRESSO Project-Team

8. Dissemination

8.1. Scientific Animation

- Jean-Pierre Talpin is Associate Editor with the ACM Transactions for Embedded Computing Systems (TECS); he is also Associate Editor with the Springer journal on Frontiers of Computer Science (FCS) and Associate Editor with EURASIP journal of embedded systems.
  Jean-Pierre Talpin co-chaired the program committee of the 12th International Symposium on Methods and Models for System Design (MEMOCODE'13).
  He served as program committee member of the International Conference on Embedded Systems (EMSOFT'13).
- Thierry Gautier served as program commitee member for the 2013 Electronic System Level Synthesis Conference, ESLsyn 2013 (http://www.ecsi.org/eslsyn2013).
- Loïc Besnard participated to the Inria stand at the EclipseCon France (Toulouse, June 2013).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Jean-Pierre Talpin taught two conference-lectures to Graduate students at the Arlington campus of Virginia Tech in April and October.
- Jean-Pierre Talpin taught a series of fifteen MooC lectures to Master students at Beihang University, in November and December.
- Adnan Bouakaz taught three courses (Operating systems organization, Java programming, functional programming) to undergraduate students at University of Rennes 1 from September to November.

8.2.2. Juries

- Thierry Gautier served on an Associate Professor selection committee of Université de Rennes 1 in May 2013.

S4 Project-Team

9. Dissemination

9.1. Scientific Animation

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

9.2.2. Supervision

9.2.3. Juries

9.3. Popularization

TRIO Team

8. Dissemination

8.1. Scientific Animation

- Liliana Cucu-Grosjean has been the Delegate of International Relations for the Inria Nancy-Grand Est center until September 1st 2013.
- Liliana Cucu-Grosjean is an elected member of Inria Evaluation Commission (CE).
- Liliana Cucu-Grosjean is head of the Inria Committee on Equal Opportunities
- Olivier Zendra is head of the Documentation Committee of Inria Nancy Grand Est (Commission IST); member of the Health, Safety and Work Environment of Inria and of Inria Nancy Grand Est - LORIA Committees (CNHSCT and CLHSCT); member of the Inria Committee on Prevention of Psycho-social Risks and Quality of Life at Work (PRPS-QVT); member of the Permanent Education Committee of Inria Nancy Grand Est - LORIA; member of the new Sustainable Development Local and National Committees; member of the Inria Nancy Grand Est - LORIA Committee for the selection of hardware configurations; member of the Inria Committee on Equal Opportunities
- Liliana Cucu-Grosjean was member of the selection committee at University of Lorraine (position 27MCF0387), University of Toulouse (position 61MCF0789) and Inria Nancy-Grand Est (CR2 contest)
- Olivier Zendra is CIR expert for the Ministry of Research for the scientific evaluation of research in companies.
- Liliana Cucu-Grosjean is an ANRT expert for evaluating CIFRE applications.
- Olivier Zendra was an expert for evaluating COFECUB applications in 2013.
- Olivier Zendra is founder and steering committee member of the ICOOOLPS (International Workshop on Implementation, Compilation, Optimization of Object-Oriented Languages, Programs and Systems) workshop, usually joint to ECOOP.
- Liliana Cucu-Grosjean is steering committee member of RTSOPS (joint workshop of ECRTS) and WMC (joint workshop of RTSS).
- Liliana Cucu-Grosjean was co-chair of RTSOPS (ECRTS 2012) and WMC (RTSS 2013) as well as co-editor of the respective proceedings.
- Liliana Cucu-Grosjean was program committee member of IEEE RTSS 2013, IEEE ETFA 2013, DATE 2013 and IEEE SIES'2013.
- Olivier Zendra was program committee chair of ICOOOLPS 2013.
- Olivier Zendra was program committee member for CIEL 2013.
- Olivier Zendra was workshop organization chair for the 3 collocated conferences ECOOP 2013, ECSA 2013 and ECMFA 2013.
- Olivier Zendra was organization committee member for CIEL 2013 (for which he was primary contact), GDRP GPL 2013 and AFDAL 2013.
- The permanent members of TRIO team are reviewers for numerous international Conferences and Workshops and, in particular for the following journals: IEEE Transactions on Industrial Informatics, Real-Time Systems, IEEE Computer Communications, Journal of Discrete Event Systems, Journal of Systems Architecture, Journal of Embedded Computing, Journal of Scheduling, Theoretical Computer Science, ACM Surveys, ACM Transactions on Embedded Computing Systems, Information Processing Letters, Science of Computer Programming.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Liliana Cucu-Grosjean, Multiprocessor real-time systems, 30h, Master (M1), University of Lorraine, France

8.2.2. Supervision

PhD & HdR :

PhD : Dorin Maxim, Probabilistic Real-Time Systems, University of Lorraine, December 10th, 2013, Liliana Cucu-Grosjean and Françoise Simonot-Lion

AOSTE Project-Team

9. Dissemination

9.1. Scientific Animation

Robert de Simone

General Chair: RTNS 2013.

Technical Program Committee: EmSoft 2013, MEMOCODE2013, FDL2013, CSDM 2013.

Board of Administrators: CIM PACA Design Platform association

Yves Sorel

Technical Program Committee: RTNS 2013, DASIP 2013

Editorial Board: Traitement du Signal Journal

Steering Committee: OCDS/SYSTEM@TIC Paris-Region Cluster

Liliana Cucu-Grosjean

Inria Evaluation Commission: elected member

Technical Program Committee: IEEE RTSS 2013, IEEE ETFA 2013, DATE 2013 and IEEE SIES'2013.

Steering Committee and co-chair: RTSOPS2013, WMC2013 (workshops)

Dumitru Potop Butucaru

Technical Program Committee: Memocode 2013, ACSD 2013, EslSyn 2013, APRES 2013

Julien Deantoni

General Chair: organizer and chair: First international workshop on globalization of modeling languages (GeMoC)

Technical Program Commitee: CIEL2013, GlobalDSL2013, Journal of System and Software

Laurent George

General Chair: ECRTS 2013

Program Committee Chair: ReTiMiCS 2013

Scientific Co-chair: ACTRISS group, supported by GDR ASR (CNRS, France) (http://www.actriss.org/).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Julien Deantoni, Computer Environnement, 30 h, L2 level, Polytech engineering school of University Nice/Sophia-Antipolis (UNS EPU) France.

Master:Julien Deantoni, Model Driven Engineering, 22 h, M2, UNS EPU.

Master : Julien Deantoni, C++ and Object Oriented Programming, 54 h, M1, UNS EPU.

Master: Julien Deantoni, Embedded Software and systems, 7 h, M2, UNS EPU.

Master: Julien Deantoni, VHDL, 40 h, M1, UNS EPU.

Licence: Sid-Ahmed-Ali Touati, Assembleurs et jeux d'instructions, 52h, L3, UNS Licence info.

Licence: Sid-Ahmed-Ali Touati, Systèmes informatiques, 30h, L1, UNS Licence info.

Master: Sid-Ahmed-Ali Touati, Programmation efficaces pour programmes embarqués et hautes performances, 16h, M1 Master ISI.

Master: Sid-Ahmed-Ali Touati, Systèmes d'exploitation avancés, 39h, M1, UNS Master ISI.

Master: Sid-Ahmed-Ali Touati, Programmation efficace et Optimisation de code, 16h, M1, UNS Master ISI.

Master: Sid-Ahmed-Ali Touati, Architecture des Processeurs, 15h, M1, UNS EPU.

Licence : Frédéric Mallet, Introduction à la Programmation Objet, 45h, L1, UNS.

Licence: Frédéric Mallet, Architecture des ordinateurs, 45h, L3, UNS.

Master: Frédéric Mallet, Programmation Avancée et Design Patterns, 93h, M1, UNS.

Master: Frédéric Mallet, Java pour l'Informatique Industrielle, 24h, M1, UNS.

Master: Frédéric Mallet, Architectures des ordinateurs, 12h, M1, UNS.

Master: Frédéric Mallet, Formal Models for Network-On-Chips, 3h, M2, UNS.

Licence : Marie-Agnes Peraldi-Frati, Algorithms and programming 60h,L1, UNS Institute of technology.

Licence : Marie-Agnes Peraldi-Frati, System and Networks administration 80h, L2, UNS Institute of technology .

Licence :Marie-Agnes Peraldi-Frati, Web Programming 50 h , L2, UNS Institute of technology.

Master : Robert de Simone, Formal Models for Networks-on-Chip, 24h , M2, UNS.

Master : Robert de Simone, Semantics of Embedded and Distributed Systems, 24 h, M1, UNS.

Master: Yves Sorel, Optimization of distributed real-time embedded systems, 24H, M2, University Paris Sud.

Master: Yves Sorel, Distributed real-time systems, 26H, M2, University Paris Est

Master: Yves Sorel, Specification and formal models for embedded systems, 28H, M2, ENSTA Engineering School Paris

Master: Yves Sorel, Correct by construction design of reactive systems, 18H, M2, ESIEE Engineering School Noisy-Le-Grand

Master: Dumitru Potop and Thomas Carle, Programmation synchrone des systèmes temps-réel, 8h, M1, EPITA Engineering School Paris

Licence: Laurent George, Java and Shell programming 48h, L1, IUT RT UPEC

Master: Laurent George, Distributed Real-Time Systems, 24h, M2, UPEC

9.2.2. Supervision

PhD: Carlos Ernesto Gomez-Cardenas,*Environnement multi-vues pour la métamodélisation sémantique formelle de systèmes embarqués*, UNS, defended Dec 20th 2013, supervised by Frédéric Mallet, co-supervised by Julien deAntoni.

PhD in progress: Matias Vara-Larsen, *Toward a formal and hierarchical timed model for concurrent heterogeneous model*, ANR/CNRS, started November 2012, supervised by Frédéric Mallet, co-supervised by Julien Deantoni.

PhD in progress: Ameni Khecharem, *High-Level modeling of hierarchical power management policies in SoCs*, UNS, started October 2012, supervised by Robert de Simone.

PhD in progress: Ying Lin, *Formal Analysis of polychronous models with MARTE/CCSL*, East China Normal University, started September 2011, supervised by Jing Liu (ECNU), co-supervised by Frédéric Mallet.

PhD in progress: Emilien Kofman, *Conception Haut Niveau Low Power d'objets mobiles communicants*, UNS, started Oct 2013, supervised by Robert de Simone, co-supervised by François Verdier (UMR CNRS/UNS LEAT).

PhD in progress: Amin Oueslati, *Modélisation conjointe d'applications et d'architectures parallèles embarqués en pratique*, UNS, started Jan 2014, supervised by Robert de Simone.

PhD in progress: Falou Ndoye, *Multiprocessor real-time scheduling taking into account preemption cost*, started January 2011, supervised by Yves Sorel.

PhD in progress: Manel Djemal, *Distributed real-time scheduling onto NoC architectures*, EDITE/UPMC, started Nov. 2010, co-supervised by Alix Munier (UPMC/Lip6) and D. Potop-Butucaru.

PhD in progress: Thomas Carle, *Real-time implementation of embedded control applications with conditional control onto time-triggered architectures*, EDITE/UPMC, started Sep. 2011, supervised by D. Potop-Butucaru.

PhD : Dorin Maxim, Probabilistic Real-Time Systems, University of Lorraine, December 10th, 2013, co-supervised by Liliana Cucu-Grosjean and Françoise Simonot-Lion

9.2.3. Juries

Robert de Simone

PhD reviewer: Adnan Bouakaz (U. Rennes 1), Jagadish Suryadevara (Malardalen U., Sweden)

HDR reviewer: Sébastien Gérard (U. Paris 11 Orsay).

Frédéric Mallet

PhD reviewer: Xin An (U. Grenoble 1), Clément Guy (U. Rennes 1)

PhD examiner: João Claudio Rodrigues Américo (U. Grenoble 1), Jair Gonzalez (Mines-Telecom)

Laurent George

PhD reviewer: Xiaoting Li (ENSEEIHT), Ahmed Daghsen (UTC Compiègne)

Yves Sorel

PhD reviewer: Yassine Ouhammou (ENSMA Poitiers)

PhD examiner: Pierre Courbin (U. Paris Est)

Dumitru Potop Butucaru

PhD reviewer: Léonard Gérard (U. Paris Sud)

9.3. Popularization

We held a thematic Spring School in late April in Shanghai, based on the topics of the DAESD associated-team 8.4.1.1 . It was open to students from all over China, and we invited also chinese speakers (but the attendance of around sixty students was mostly from several universities in and around Shanghai).

CONVECS Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Software Dissemination and Internet Visibility

The CONVECS project-team distributes several software tools: the CADP toolbox (see § 5.1), the TRAIAN compiler (see § 5.2), the PIC2LNT translator (see § 5.3), and the PMC model checker (see § 5.4). In 2013, the main facts are the following:

- We prepared and distributed 11 successive versions (from 2013-a to 2013-l "Zurich") of CADP.
- We were requested to grant CADP licenses for 934 different computers in the world.
- We released version 3.0 of the PIC2LNT translator from an applied π-calculus to LNT in May 2013.
- We released version 1.0 of the PMC partial model checker for networks of automata in May 2013.

The CONVECS Web site [14] was updated with scientific contents, announcements, publications, etc.

By the end of December 2013, the CADP forum [15], opened in 2007 for discussions regarding the CADP toolbox, had over 270 registered users and over 1400 messages had been exchanged.

Other research teams took advantage of the software components provided by CADP (e.g., the BCG and OPEN/CAESAR environments) to build their own research software. We can mention the following developments:

- Formal verification of BPMN models with the Alvis modeling language [64], [65], [66]
- The DFTCalc tool for efficient fault tree analysis [29], [28]
- Efficient modeling, generation, and analysis of Markov automata [67]
- Modeling and verification techniques for the incremental development of UML architectures [63]
- Model based design of complex embedded systems [27]
- Model extraction approach to verifying concurrent C programs [40]
- Model checking based approach to automatic test suite generation for Web services and BPEL [73]
- The VIP Design graphical language for the design of image and video processing embedded systems [74], [75]
- Active learning of extended finite state machines [69]
- Incremental construction and interoperability analysis of critical systems [56], [55], [62]
- Modeling robot behavior with CCL [54]
- Behavioural verification of distributed components [52]
- Efficient property preservation checking of model refinements [71]
- Efficient operational semantics for EB3 for verification of temporal properties [70]
- Multilevel contracts for trusted components [59]

Other teams also used the CADP toolbox for various case studies:

- Formally reasoning on a reconfigurable component-based system [48]
- Assisting refinement in system-on-chip design [60]
- Formal development of control software in the medical systems domain [61]
- Model-driven approach supporting formal verification for Web service composition protocols [38]
- Scalably verifiable cache coherence [72]
- Improved test case generation from UML statecharts [34], [33]

[14] http://convecs.inria.fr
[15] http://cadp.inria.fr/forum.html

9.1.2. Program Committees

In 2013, the members of CONVECS took on the following responsibilities:

- H. Garavel is an editorial board member of STTT (*Springer International Journal on Software Tools for Technology Transfer*).
- F. Lang is an editorial board member of the Scientific World Journal in the Computer Science subject area.
- G. Salaün is an editorial board member of SOCA (*Springer International Journal on Service Oriented Computing and Applications*).
- G. Salaün is a steering committee member of FACS (*International Symposia on Formal Aspects of Component Software*).
- G. Salaün is a steering committee member of FOCLASA (*International workshops on Foundations of Coordination Languages and Self-Adaptive Systems*).
- G. Salaün was a program committee member for MODELSWARD'2013 / MODA'2013 (*1st International Conference on Model-Driven Engineering and Software Development, Special Session on Model-Driven Software Adaptation*), Barcelona, Spain, February 19–21, 2013.
- G. Salaün was a program committee member for SAC'2013 (*28th Annual ACM Symposium on Applied Computing, Track on Service-Oriented Architectures and Programming*), Coimbra, Portugal, March 18–22, 2013.
- G. Salaün and W. Serwe were program committee members for FSEN'2013 (*5th International Conference on Fundamentals of Software Engineering*), Tehran, Iran, April 24–26, 2013.
- G. Salaün was a program committee member for CBSE'2013 (*16th International ACM Sigsoft Symposium on Component-Based Software Engineering*), Vancouver, Canada, June 18–20, 2013.
- G. Salaün was a program committee member for QASBA'2013 (*2nd International Workshop on Quality Assurance for Service-based Applications*), Lugano, Switzerland, July 15, 2013.
- F. Lang was a program committee member for ETR'2013 (*Ecole d'été Temps-réel*), Toulouse, France, August 26–30, 2013.
- F. Lang was a program committee member for ESOCC'2013 (*European Conference on Service-Oriented and Cloud Computing*), Málaga, Spain, September 11–13, 2013.
- F. Lang and R. Mateescu were program committee members for FMICS'2013 (*18th International Workshop on Formal Methods for Industrial Critical Systems*), Madrid, Spain, September 23–24, 2013.
- G. Salaün was a program committee member for FACS'2013 (*10th International Symposium on Formal Aspects of Component Software*), Nanchang, China, October 28–30, 2013.

9.1.3. Awards and Distinctions

H. Garavel is an invited professor at Saarland University (Germany) as a holder of the Gay-Lussac Humboldt Prize.

9.1.4. Lectures and Invited Conferences

- H. Garavel attended the Dagstuhl Seminar #13051 on "*Software Certification: Methods and Tools*" (Schloss Dagstuhl, Germany, January 27 – February 1st, 2013). He gave a lecture entitled "*A Naive Look at Software Certification Practices – and Proposals for Enhancement*" on January 30, 2013.
- G. Salaün visited the University of Málaga (Spain) from February 2 to March 8, 2013. He gave a talk entitled "*Formal Methods for Cloud Computing Environments*" on February 6, 2013 and a talk entitled "*Verification of Contract-based Communicating Systems*" on February 13, 2013.
- H. Garavel visited RWTH Aachen (Germany) on February 25–28, 2013. He gave a talk entitled "*CAESAR Nets, NTIF, and FIACRE: Better than Slim, and also Faster?*".

- G. Salaün gave a keynote lecture entitled "*Verification of Contract-based Communicating Systems*" at GRAPHITE'2013 (Rome, Italy) on March 24, 2013.
- H. Garavel was invited to the seminar "*25 Years of Combining Compositionality and Concurrency*" (Königswinter, Germany, August 7–9, 2013). He gave a lecture entitled "*25 Years of Compositionality Issues in CADP: An Overview*".
- F. Lang gave a lecture entitled "*CADP: A Toolbox for the Construction and Analysis of Distributed Processes*", followed by a lab session on CADP at ETR'2013 (Toulouse, France) on August 28, 2013.
- F. Lang gave a keynote lecture entitled "*Langage de nouvelle génération pour la modélisation et vérification formelle de systèmes asynchrones*" at JDEV'2013 (Palaiseau, France) on September 4, 2013.
- H. Garavel gave a lecture entitled "*25 Years of Combining Compositionality and Concurrency*" at Saarland University on December 20, 2013.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

CONVECS is a host team for the computer science master entitled "*Mathématiques, Informatique, spécialité : Systèmes et Logiciels*", common to Grenoble INP and University Joseph Fourier.

In 2013, we carried out the following teaching activities:

- G. Salaün is co-responsible for the ISI (*Ingéniérie des Systèmes d'Information*) department of ENSIMAG since September 1, 2011.
- H. Evrard served as a teaching assistant in a course on "*Algorithmique et structures de données*", given by Frédéric Wagner to the first year computer science engineering students of ENSIMAG (36 hours).
- H. Evrard served as a teaching assistant in a course on "*Introduction aux réseaux de communication*", given by Roland Groz to the first year computer science engineering students of ENSIMAG (18 hours).
- H. Evrard served as a teaching assistant in a course on "*Systèmes d'exploitation et programmation concurrente*", given by Yves Denneulin to the second year computer science engineering students of ENSIMAG (18 hours).
- A. Kriouile served as a teaching assistant in a course on "*Conception de circuits et architectures des ordinateurs*", given by Frédéric Pétrot to the first year computer science engineering students of ENSIMAG (27 hours).
- A. Kriouile served as a teaching assistant in a course on "*Introduction aux réseaux de communication*", given by Roland Groz to the first year computer science engineering students of ENSIMAG (36 hours).
- A. Kriouile served as a teaching assistant for a student project "*Projet logiciel en C*", proposed by François Broquedis and Matthieu Chabanas to the first year computer science engineering students of ENSIMAG (20 hours).
- F. Lang and W. Serwe gave a course on "*Spécification et vérification de systèmes concurrents et temps-réel*" to the third year computer science engineering students of ENSIMAG (18 hours).
- G. Salaün gave a course on "*Algorithmique parallèle et orientée-objet*" to the second year computer science engineering students of ENSIMAG (36 hours).
- L. Ye gave a course on "*Théorie des langages*" to the first year computer science engineering students of ENSIMAG (10 hours).

9.2.2. Juries

- R. Mateescu was a panel member for Syed Hussein Syed Alwi's PhD thesis, entitled "*Vérification compositionnelle pour la conception sûre de systèmes embarqués*", defended at Université Pierre et Marie Curie, Paris, France, on July 11, 2013.
- G. Salaün was a panel member for Huu Nghia Nguyen's PhD thesis, entitled "*A Symbolic Approach for the Verification and the Testing of Service Choreographies*", defended at Université Paris Sud, Orsay, France, on October 30, 2013.

9.3. Popularization

H. Garavel participated to the committee in charge of organizing the Aerospace Valley series of industrial conferences on formal methods. The second conference [16] [17], devoted to static analysis, held on June 28, 2013 in Toulouse and retransmitted by video-conference in Grenoble, attracted 95 participants from industry and academia.

R. Mateescu was in charge of the scientific organization of the In'Tech seminar entitled "*Formal Validation of Industrial Critical Systems*" held on April 18, 2013 at the Inria Grenoble – Rhône-Alpes research center in Montbonnot. The seminar attracted about 100 participants from academia and industry. F. Lang gave a public demonstration of the CADP tools and R. Mateescu gave a talk entitled "*Formal Modeling and Verification of Concurrent Systems using CADP*".

9.4. Miscellaneous Activities

H. Evrard is a member of the council of the MSTII doctoral school.

H. Evrard and G. Salaün are members of the council of the LIG laboratory.

H. Garavel is a member of the LIG commission in charge of preparing candidates selected for recruitment interviews at CNRS.

H. Garavel is a member of the operational committee of the EMSOC cluster ("Embedded System on Chip") within the "*pôle de compétitivité*" Minalogic.

H. Garavel was a reviewer for various ongoing ANR (*Agence Nationale de la Recherche*) projects evaluated in 2013.

F. Lang is a member of the "*commission du développement technologique*", which is in charge of selecting R&D projects for Inria Grenoble - Rhône-Alpes.

E. Léo and W. Serwe are members of the "*comité de centre*" of Inria Grenoble - Rhône-Alpes.

R. Mateescu is the correspondent of the "*Département des Partenariats Européens*" for Inria Grenoble - Rhône-Alpes.

G. Salaün is a member of the scientific council of Grenoble INP (*Conseil scientifique de l'institut*).

H. Garavel is "*chargé de mission*" of the LIG laboratory and responsible for the liaison with Minalogic.

W. Serwe is "*chargé de mission*" of the LIG laboratory for the scientific axis "*Formal Methods, Models, and Languages*".

[16] http://www.inria.fr/centre/grenoble/agenda/forum-methodes-formelles
[17] http://www.inria.fr/centre/grenoble/actualites/fiabilite-des-logiciels-pas-uniquement-pour-les-avions

Hycomes Team

7. Dissemination

7.1. Scientific Animation

Benoît Caillaud has served in the steering and program committees of the International Conference on Application of Concurrency to System Design (ACSD'13) and of the Applications of Regions Theory (ART'13) satellite workshop. He is serving on the Evaluation Committee of INRIA.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Benoît Caillaud has contributed to the training programme for the computer-science option of the *agrégation* in mathematics, at ENS Cachan-Ker Lann.

7.2.2. Supervision

PhD in progress Ayman Aljarbooh, *Scalable Simulation of Hybrid Systems: Language Design and Compilation*, started December 2013, supervised by Benoît Caillaud

7.2.3. Juries

Benoît Caillaud has participated to the jury for the defense of Florent Avellaneda's PhD thesis, *Verification of stateful Petri-nets under a partial order semantics*, December 10th 2013, Aix-Marseille University. He has also served on the junior researcher hiring committee of Inria Sophia Antipolis - Méditerranée

MUTANT Project-Team

9. Dissemination

9.1. Scientific Animation

MuTant acted as co-organizer and scientific chair for the first International Conference on Geometric Science of Information 2013 which took place in École des Mines (Paris) in partnership with SEE, and THALES. The conference attracted more than 150 participants worldwide and conference proceedings were published by Springer. MuTant team members organized a special session on Audio and Music and further organized a special social session on music computing at Ircam.

The Brillouin Seminar series on Information Geometry is coordinated by MuTant in partnership with LIX and THALES. It gathers 80 international researchers on the topic from various disciplines. In 2013, we organized 4 major talks. The seminar activity on 2013 was particularly down due to the co-organization of the first International Conference on the topic by MuTant and collaborators. Videos are available on the seminar website.

Jean-Louis Giavitto is in the management team of the GDR GPL (Genie de la programmation et du logiciel), responsible with Etienne Moreau of the “Languages and Ve´rification” pole of the GDR. He is also and expert for the ANR DEFI projects and a reviewer for FET projects for the UC. He is also the redactor-in-chief of TSI (Technique et Science Informatiques) published by Lavoisier.

Jean-Louis Giavitto has participated in the program committee of the following workshop and conferences: Rencontres interdisciplinaires de Rochebrune: ”La preuve et ses moyens” 13 au 19 janvier 2013; Digital Entertainment Technologies and Arts (DETA) track at GECCO 2013, 6-10 July 2013, Amsterdam, The Netherlands NICSO 2013 The VI International Workshop on Nature Inspired Cooperative Strategies for Optimization, September 2-4, 2013 Canterbury, United Kingdom; HaPoC 2013 2nd International Conference on the History and Philosophy of Computing 2013. 28th - 31st October 2013, 27/11/13 4/9 Ecole Normale Superieure, Paris; MeCBIC 2013 7th Workshop on Membrane Computing and Biologically Inspired Process Calculi, 7th July 2013, Riga, Latvia.

Jean-Louis Giavitto was cochair of the 6th Spatial Computing Workshop, satellite workshop of AAMAS 2013, Saint-Paul, USA.

Arshia Cont participated in the following events: Course in Collège de France, Informatics of Time and Events curated by Gérard Berry, June 2013; Invited keynote in Seoul (South Korea) on Antescofo, November 2013; Keynote in GSI, Grenoble in December 2013; Invited speech and demonstration for the 20th anniversary of Prix La Recherche; CHI workshop on Models of Time with Jean-Louis Giavitto and Florent Jacquemard, April 2013.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Arshia Cont, Audio Technology Review, 2h/week, L3, Paris Superior Conservatory of Music (CNSMDP), France.

Master : Arshia Cont, Machine Learning for Music, 15 hours, M2, UPMC/ATIAM, France.

Doctorat : Enseignant, titre du cours, nombre d’heures en équivalent TD, université, pays

Jean-Louis Giavitto has been invited to give a one week course on Spatial Computing at the University of Cali, Colombia (20 hours).

9.2.2. Supervision

PhD in progress :

Jose´ Echeveste, Synchronous Languages for Computer Music Composition and Performance, Started September 2011, co-directed by Jean-Louis Giavitto and Arshia Cont.

Philippe Cuvilier, Inference Mechanisms for on-line Machine Listening, Started September 2013, directed by Arshia Cont

Clement Poncelet, Formal analysis of human-machine interactions in complex timed scenarios. Started in October 2013, directed by Florent Jacquemard.

9.2.3. Juries

Florent Jacquemard participated in the selection committee to the 2013 recruitment campaign at the Inria center of Lille.

Florent Jacquemard participated to the defense committee for the PhD of Vincent Hugot, “Tree Automata, Approximations, and Constraints for Verification, Tree (Not-Quite) Regular Model-Checking”, University of Franche-Comté, September 2013. and to the mid-term PhD defense of Emil Mircea Andriescu on “Dynamic synthesis and deployment of mediation protocols in collaborative mobile environments”, a CIFRE agreement between UPMC, Inria and the SME Ambientic, in November 2013.

Jean-Louis Giavitto has expertised several project for the Ulysses Network http://www.ulysses-network.eu/web/home/; and has been reviewer of the PhD thesis of M. Obrovac (IRISA), A. Ajouli (LINA) and of the Habilitation of Arnaud Banos (Sorbonnes). He was also member of one selection committee for UPMC.

9.3. Popularization

MuTant team was featured in the 2nd edition of Made In France (MIF) Expo in the major Exhibition Hall in Paris (Porte de Versaille) with a dedicated stand for Antescofo with more than 3 million visitors during 3 days.

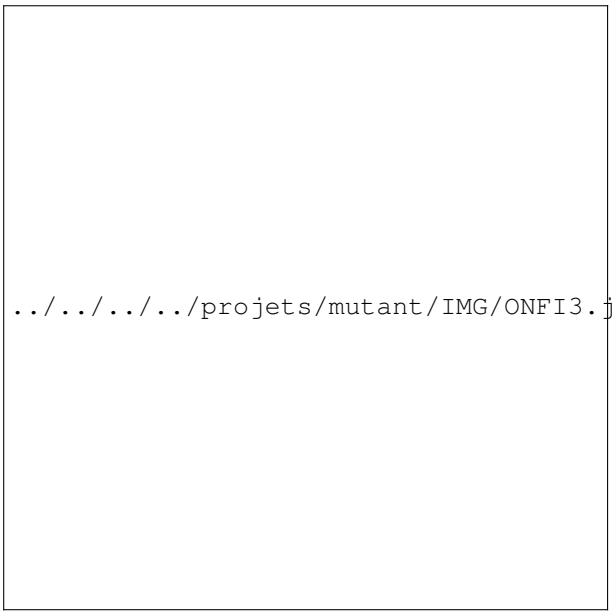

Figure 6. Antescofo demo in Ministry of Industry featuring Marlène Schaff (French THE VOICE, Season 2)

Antescofo was featured by the French Ministry of Industry for a public talk and largely diffused demo featuring the french star singer Marlène Schaff from *The Voice*.

Arshia Cont was invited for a public presentation/demo of *Antescofo* for the 20th anniversary of the Prix La Recherche. Click for video.

Jean-Louis Giavitto has co-animated the public discussion following the movie "Codebreaker: Alan Turing" with C. Villani and G. Berry at the Cinema Grand Action. He gave several seminars for a non computer scientist audience:

> "Analyse formelle des concepts, Q-analyse et programmation spatiale : quelques aspects philosophiques du nœud mathématique/musique/ informatique, séminaire MaMuPhi, l'Ecole Normale (february 2013);
>
> "Écriture du temps et de l'interaction en informatique musicale", séminaire Philosophie de l'informatique, de la logique et de leurs interfaces, Centre Cavaillès, Ecole Normale, (mars 2013);
>
> "Modélisation spatiale et approche géométrique en musique", Journées nationales du RNSC (octobre 2013);
>
> "Simultanéité, succession et durée dans l'interaction musicale en temps-réel", séminaire MaMux Temps, rythme et arithmétique, (décembre 2013).
>
> As the redactor-in-chief of TSI, Jean-Louis Giavitto has initiated a new section devoted to portraits and talking with french personalities in computer science. These articles are also published in the SIF journal.

José Echeveste has presented Antescofo and participed to the event organized for the "Fête des Sciences" at Forum des Halles and UPMC.

We have published a popularization article on "Computer Assisted Music" in the review DocSciences, number 15.

PARKAS Project-Team

9. Dissemination

9.1. Scientific Animation

- Albert Cohen was the program chair of CC 2014, the TPC chair of the DAC 2013 and 2014 ESS1 subcommittees, and the co-Program Chair of the APPT 2013 bi-annual Symposium on Advanced Parallel Processing Technology. Albert Cohen was also a member of the PC of PLDI 2014, and a member of the ERC of ASPLOS 2014, PPoPP 2014 and ICS 2014. Albert Cohen also participated to the PC of the IMPACT and HiRES workshops associated with HiPEAC 2014.
- Albert Cohen is an associate editor of ACM TACO and IJPP (Springer).
- Albert Cohen will be the general chair of PPoPP 2015.
- Albert Cohen was the sponsor chair for the HiPEAC 2013 and HiPEAC 2014 conference, and will serve as the exhibit and sponsor chair for HiPEAC 2015.
- Marc Pouzet was a member of the PC of DAC 2014, AFADL 2014, MSR 2013, RTNS 2013, DATE 2013.
- Marc Pouzet manages with Catherine Dubois (ENSIIE, Evry, France) the GDR (“Groupe de Recherche”) TLP (“Types, Langages et Preuves”) du CNRS (“Centre National de Recherche Scientifique”). Two one-day seminars are organised every year.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: T. Bourke & J. Vuillemin, “Digital Systems”, 64h, L3, Ecole normale supérieure, France

Licence: L. Mandel, “Systèmes”, 42h, L3, Université Pars-Sud 11, France

Licence: L. Mandel & M. Pouzet, “Systèmes et réseaux”, 24h+24h, L3, Ecole normale supérieure, France

Licence: L. Mandel, “Langages de programmation et compilation”, 24h, L3, Ecole normale supérieure, France

Master: L. Mandel & M. Pouzet, “Synchronous Systems”, 8h+16h, M2, MPRI: Ecole normale supérieure and Université Paris Diderot, France

Master: A. Cohen & F. Zappa Nardelli, “Semantics, languages and algorithms for multicore programming”, 9h+14h, M2, MPRI: Ecole normale supérieure and Université Paris Diderot, France

Licence: “Components of a Computing System Introduction to Computer Architecture and Operating Systems” (L3), A. Cohen (44h), École Polytechnique, France

Master 1 École Polytechnique: “Operating Systems Principles and Programming” (M1), A. Cohen (38h), École Polytechnique, France

Marc Pouzet is supervising the national entry exam in computer science for École normale supérieure.

Marc Pouzet is director of studies (“Directeur des études”) for the CS department of École normale supérieure.

9.2.2. Supervision

PhD : Léonard Gérard, Programmer le parallélisme avec des futures en Heptagon un langage synchrone flot de données et étude des réseaux de Kahn en vue d’une compilation synchrone, Université Paris-Sud 11, Orsay. Soutenue le 25 septembre 2013, au LRI, à Orsay.

PhD : Cédric Pasteur, Raffinement temporel et exécution parallèle dans un langage synchrone fonctionnel, Université Pierre et Marie Curie (UPMC), soutenue le 26 novembre 2013, au Collège de France. Encadrants: Louis Mandel et Marc Pouzet.

PhD in progress : Guillaume Baudart, Real-time fidelity in Quasi-synchronous Systems, Start: 1/10/2013, Timothy Bourke and Marc Pouzet

PhD in progress : Robin Morisset, Compiler Optimisations and Concurrency, 1/10/2013, F. Zappa Nardelli

9.2.3. Juries

- Albert Cohen was the president of the Habilitation Thesis committee of Fabien Coelho, MINES ParisTech.
- Albert Cohen was the president of the PhD thesis committee of Bruno Bodin, UPMC (CIFRE Kalray).
- Albert Cohen was a reviewer for the PhD thesis of Martin Schindewolf at the Karlsruhe Institute of Technology.
- Albert Cohen was a reviewer for the PhD thesis of Daniel Cordes at TU Dortmund.
- Albert Cohen was a reviewer for the PhD thesis of Yuriy Kashnikov, UVSQ.
- Albert Cohen was an examiner in the PhD thesis committee of Thomas Preud'Homme, UPMC.
- Marc Pouzet was a reviewer for the PhD thesis of Boris Golden, École Polytechnique.
- Marc Pouzet was a reviewer for the PhD thesis of Gideon Smeding, Université de Grenoble.
- Albert Cohen was a member of a hiring committee for professors at the University of Strasbourg.
- Albert Cohen was a member of a hiring committee for assistant professors (“maître de conférences”) at the University Claude Bernard de Lyon.

SPADES Team

9. Dissemination

9.1. Scientific Animation

- Pascal Fradet served in the program committees of MODULARITY 2014 and of JFLA 2013 and JFLA 2014 (Journées Francophones des Langages Applicatifs).
- Alain Girault served in the program committees of the international conferences DAC 2013 and MSR 2013.
- Gregor Goessler served in the program committees of the international conferences Component-Based Software Engineering (CBSE) 2013 and Design, Automation, and Test in Europe (DATE) 2014 and the workshop Hybrid Systems and Biology (HSB) 2013.
- Jean-Bernard Stefani is the current Chair of IFIP Working Group WG6.1, that sponsors the international conference series DAIS, FORTE, ICTSS, and Middleware. He is the current chair of the FORTE Steering Committee and a member of the DISCOTEC joint international conference (hosting Coordination, DAIS and FORTE).

9.2. Teaching - Supervision - Juries

9.2.1. Supervision

PhD: Quentin Sabah, "Simple Isolation for An Abstract Actor Machine", Grenoble University, 4/12/2013, advised by Jean-Bernard Stefani.

PhD: Gideon Smeding, "Verification of Weakly-Hard Requirements on Quasi-Synchronous Systems", Grenoble University, 19/12/2013, co-advised by Gregor Goessler and Joseph Sifakis.

PhD in progress: Vagelis Bebelis, "Advanced dataflow programming for embedded systems", Grenoble University, since 12/2011, co-advised by Pascal Fradet and Alain Girault.

PhD in progress: Dmitry Burlyaev, "Specification and synthesis of fault-tolerant circuits", Grenoble University, since 12/2011, co-advised by Pascal Fradet and Alain Girault.

PhD in progress: Yoann Geoffroy, "Towards a general causality analysis framework", Grenoble University, since 10/2013, co-advised by Gregor Goessler and Daniel Le Métayer (Privatics INRIA team).

9.2.2. Juries

- Alain Girault was referee for the PhD thesis of Hervé Yviquel (University of Rennes 1) and for the PhD thesis of Léonard Gérard (University of Orsay).
- Jean-Bernard Stefani was referee for the PhD thesis of Cédric Pasteur (University of Paris VI).

FORMES Team

8. Dissemination

8.1. Scientific Animation

Frédéric Blanqui was member of the Steering Committee of the International Conference on Rewriting Techniques and Applications (RTA) for 3 years until June 2013.

Frédéric Blanqui was invited to present his work on "the formalization of λ-calculus and Tait-Girard's notion of computability" at the 3rd Workshop on Proof Theory and Rewriting (PR), March 2013, Kanazawa, Japan.

Vania Joloboff has organized a LIAMA Open Day in Shanghai in May 2013, in collaboration with East China Normal University.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Frédéric Blanqui organized a 7-days school at the Institute of Applied Mechanics and Informatics (IAMA) of the Vietnamese Academy of Sciences and Technology (VAST) at Ho Chi Minh City, Vietnam, from 12 to 19 March 2013. The mornings were dedicated to theoretical lectures introducing basic notions in mathematics and logic for the analysis of computer programs. The afternoons were practical sessions introducing the OCaml programming language and the Coq proof assistant. Lecture notes are given in [17].

Vania Joloboff has taught simulation seminars at Shenzhen Institutes of Advanced Technology.

Licence: Jean-François Monin, Introduction to Interactive Proof of Software, 50 hours, L3, Tsinghua University, China
This course is expected to attract students in the FORMES group via the local PhD program; already one of them (2009) is currently a PhD student of Jean-Pierre Jouannaud, another (2010) in is the PhD track with Gu Ming and 2 others (2010) work with Jean-François Monin and Vania Joloboff.

Doctorate: Jean-François Monin (organizer and teacher), Coq Summer School, 30 hours, Tsinghua University, China

8.2.2. Supervision

PhD : Xiaomu Shi, "Certification of an Instruction Set Simulator", University of Grenoble, July 2013, [14] Jean-François Monin, Vania Joloboff.

PhD in progress: Kim-Quyen Ly, automated formal verification of termination certificates, October 2011, Frédéric Blanqui

PhD in progress : Jiaxiang Liu, Testing Confluence via Critical Pairs, 2012, École Polytechnique, Jean-Pierre Jouannaud

PhD in progress: Qian Wang, CoqMTU: a secure combination of the Calculus of Construction, inductive types, universes and built-in equality, 2011, École Polytechnique, Jean-Pierre Jouannaud

8.2.3. Juries

Frédéric Blanqui has been in the jury of Zhiwu Xu for his PhD on "Parametric Polymorphism for XML Processing Languages" (directors: Giuseppe Castagna and Haiming Chen).

Frédéric Blanqui refered the habilitation thesis of René Thiemann (Innsbrück University) on "A Formalization of Termination Techniques in Isabelle/HOL".

Jean-François Monin has been in the jury of Xiaomu Shi (see above).

Vania Joloboff has been in the jury of Xiaomu Shi (see above).

SECSI Project-Team

8. Dissemination

8.1. Scientific Animation

Administrative charges:

- Hubert Comon-Lundh is member of the “comité de pilotage”, labex Digicosme.
- Hubert Comon-Lundh is member of the “commission formation”, labex Digicosme.
- Hubert Comon-Lundh is member of the “Jury prix de these Gilles Kahn/SIF”.
- Hubert Comon-Lundh is member of the jury “appel à projets Digiteo”
- Hubert Comon-Lundh is member of the Master MPRI studies committee and director of the MPRI until sept. 2013.
- Stéphanie Delaune has been a member of the scientific committee of Inria Saclay since February 2012.
- Stéphanie Delaune has been “Déléguée aux thèses” at the École Doctorale Sciences Pratiques at ENS Cachan since September 2012.
- Jean Goubault-Larrecq is in charge of computer science questions, common Ecole Polytechnique-ENS Paris, Lyon, Cachan-ESPCI entrance competitive exam, starting September 2012.

Editorial boards:

- Hubert Comon-Lundh is associate editor of the ACM Transactions on Computational Logic.

Participation to program committes of conferences:

- 16th International Conference on Foundations of Software Science and Computation Structures FoSSaCS’13, Rome, Italy, March 2013 (Jean Goubault-Larrecq).
- 24th International Conference on Automated Deduction (CADE), Lake Placid, New York, USA, 2013 (Stéphanie Delaune)
- 26th IEEE Computer Security Foundations Symposium (CSF), Tulane University, New Orleans LA, USA, 2013 (Stéphanie Delaune)
- 24th International Conference on Rewriting Techniques and Applications (RTA), Eindhoven, The Netherlands, 2013 (Stéphanie Delaune)
- 20th Workshop on Logic, Language, Information and Computation (WoLLIC), Darmstadt, Germany, 2013 (Stéphanie Delaune)
- Worshop *Formal and Computational Cryptography (FCC)*, president of the program commitee. June 30, 2013, New Orleans (Hubert Comon-Lundh).
- Workshop on *Logical Frameworks and Meta-Languages: Theory and Practice* LFMTP’13, Boston, U.S.A., September 2013 (David Baelde).
- Workshop on *Fixed Points in Computer Science* FICS’13, Torino, Italy, September 2013 (David Baelde).
- 24th Journées Francophones des Langages Applicatifs JFLA’13, Aussois, France, February 2013 (David Baelde).

Organization of conferences:

- Workshop on *Fixed Points in Computer Science* FICS’13, Torino, Italy, September 2013 (David Baelde).
- 25th Journées Francophones des Langages Applicatifs JFLA’14, Fréjus, France, January 2014 (David Baelde).

Selection committees:

- Hubert Comon-Lundh was president of the "Maitre de Conférences" selection committee, ENS Paris, 2013.
- Hubert Comon-Lundh was member of the selection committee of "Maitre de conférences" selection committee, Univ. Paris-Diderot, 2013.
- Hubert Comon-Lundh was member of the Inria Paris-Rocquencourt junior researche selection committee, 2013.
- Jean Goubault-Larrecq was member of the Inria Saclay-Ile-de-France junior researcher selection committee, 2013.

Scientific boards:

- Hubert Comon-Lundh, CNRS INSII, Oct. 2010-Oct 2014
- Hubert Comon-Lundh, scientific committee, labex CPU.
- Hubert Comon-Lundh, scientific committee, LIPN.
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes
- Jean Goubault-Larrecq, member of the scientific committee of the Labex "Fondation Sciences Mathématiques de Paris".
- Jean Goubault-Larrecq, member of the scientific committe of the "Ecole de Printemps d'Informatique Théorique" (EPIT).

Invited talks:

- Hubert Comon-Lundh, *LICS: Logic in Computer Security*, invited tutorial, IEEE Symp. Logic in Computer Science, New Orleans, July 2013.
- Jean Goubault-Larrecq, *A few Pearls in the Theory of Quasi-Metric Spaces*, semi-plenary talk, Summer Topology Conference, North Bay, Ontario, Canada, July 23-26, 2013.
- Jean Goubault-Larrecq, *A Simple Proof of the Schröder-Simpson Theorem*, session on Asymmetric Topology, Summer Topology Conference, North Bay, Ontario, Canada, July 23-26, 2013.
- Jean Goubault-Larrecq, *A Constructive Proof of the Topological Kruskal Theorem*, Mathematical Foundations of Computer Science (MFCS), IST Austria, near Vienna, Austria, August 26-30, 2013.
- Jean Goubault-Larrecq, *Is Mathematical Rigor Needed in Intrusion Detection?*, Foundations and Practice of Security (FPS), La Rochelle, France, October 21, 2013.

Invitation to seminars:

- Hubert Comon-Lundh, *Towards Unconditonal Soundness*, IRISA, Rennes, Feb 1, 2013.
- Hubert Comon-Lundh, *Computationally Sound Automated Proofs of Security*, LRI, Orsay, March 15, 2013.
- Jean Goubault-Larrecq, *Orchids, ou: de l'importance de la sémantique*, séminaire DGA Innosciences, DGA, Bagneux, June 25, 2013.
- Jean Goubault-Larrecq, *Full Abstraction for Non-Deterministic and Probabilistic Extensions of PCF*, Pierre-Louis Curien Festschrift, Venice, Italy, September 9-11, 2013.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence :

- Rémy Chrétien, *Initiation à l'informatique* (TP), 39h., L1, Université Paris 7, Paris, France
- Hubert Comon-Lundh *Logic and Computability*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Programming*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Logic and Computer Science* (a.k.a., the lambda-calculus), 36h., L3, ENS Cachan and ENS Paris, France
- Jean Goubault-Larrecq, Internship reviews, 4h., L3, ENS Cachan, France
- David Baelde, *Logic and Computer Science*, 24h., L3, ENS Cachan, France
- David Baelde, *Logic II*, 22.5h., L3, ENS Cachan, France
- David Baelde, *Programming II*, 22.5h., L3, ENS Cachan, France
- David Baelde, Internship reviews, 3h., L3, ENS Cachan, France

Master :

- Jean Goubault-Larrecq, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 1/3, 3h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Stéphanie Delaune, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 2/3, 3h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Jean Goubault-Larrecq, *Advanced Complexity*, 42h., M1, MPRI course 1-17, France
- David Baelde, *Software Engineering Project*, 30h., M1, ENS Cachan, France
- Jean Goubault-Larrecq, Internship reviews, 4h., M1, ENS Cachan, France
- Hubert Comon-Lundh, Internship reviews, 32h, M2 MPRI
- Jean Goubault-Larrecq, Internship reviews, 16h., M2, MPRI, France
- Hubert Comon-Lundh *Preparation option info agreg: logique*, 24h, préparation à l'agrégation de Mathématiques, Jan-May 2012, ENS Cachan, France
- Hubert Comon-Lundh, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France
- Hubert Comon-Lundh, *Tree Automata*, M1, MPRI, 22h
- Jean Goubault-Larrecq, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France

8.2.2. Supervision

PhD in progress :

- Rémy Chrétien, *Trace equivalence for an unbounded number of sessions*, Started Oct. 2012, supervised by Stéphanie Delaune and Véronique Cortier
- Lucca Hirschi, *Reduction techniques for equivalence-based properties*, Started Sep. 2013, supervised by David Baelde and Stéphanie Delaune
- Guillaume Scerri, *Preuves abstraites de protocoles cryptographiques concrets*, Started Oct. 2011, supervised by Hubert Comon-Lundh

8.2.3. Juries

- PhD:

  - Jean Goubault-Larrecq, member of the jury: Rémi Bonnet, *Decidability and Undecidability in Vector Addition Systems with one (or more !) Zero-Tests*, ENS Cachan, January 22, 2013.
  - Jean Goubault-Larrecq, president of the jury: Song Fu, *On Pushdown Systems Model Checking: Application to Malware Detection and Software Model-Checking*, U. Paris Diderot, April 12, 2013.
  - Jean Goubault-Larrecq, president of the jury: Alexis Goyet, *The $\lambda\overline{\lambda}$-calculus, A Dual Calculus for Unconstrained Strategies*, U. Paris Diderot, December 11, 2013.
  - Jean Goubault-Larrecq, member of the jury: David Cadé, *Imple´mentations de protocoles cryptographiques prouve´es dans le mode`le calculatoire*, U. Paris Diderot, December 16, 2014.
  - Jean Goubault-Larrecq, member of the mid-term evaluation jury: Pablo Rauzy, SupTelecom Paris Tech, December 4, 2013.
- HdR:
  - Hubert Comon-Lundh, president of the jury: Jérôme Leroux. *Presburger Counter Machines*, Bordeaux, Dec.6, 2012.
  - Jean Goubault-Larrecq, reviewer and member of the jury: Michele Pagani, *Some Advances in Linear Logic*, U. Paris Nord Villetaneuse, December 5, 2013.
  - Jean Goubault-Larrecq, reviewer and member of the jury: Michele Pagani, *Some Advances in Linear Logic*, U. Paris Nord Villetaneuse, December 5, 2013.

8.3. Popularization

- Stéphanie Delaune, member of the scientific mediation committee at Inria Saclay. (“Mediation” is the new name for popularization.)
- Rémy Chrétien and Stéphanie Delaune, *La protection des informations sensibles*, article in *Pour La Science*, Nov. 2013.

ABSTRACTION Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Academy Members, Professional Societies

Patrick Cousot is a member of the Academia Europaea.

Patrick Cousot is member of the IFIP working group WG 2.3 on programming methodology.

Patrick Cousot is a member of the Board of Trustees and of the Scientific Advisory Board of the IMDEA(Instituto madrileño de estudios avanzados—Research Institute in Software Development Technology), Madrid, Spain and of the Asian Association for Foundations of Software (AAFS).

9.1.2. Collective Responsibilities

Jérôme Feret and Xavier Rival are members of the lab council of the Laboratoire d'Informatique de l'École normale supérieure.

Jérôme Feret was a member of the *comité de sélection* (hiring committee) to hire an assistant professor at the Université de Lille 1.

Antoine Miné was a member of the *comité de sélection* (hiring committee) to hire an assistant professor at the École normale supérieure (Paris).

9.1.3. Editorial Boards and Program Committees

— Patrick Cousot is member of the advisory board of the Higher-Order Symbolic Computation journal (HOSC, Springer) and of the Journal of Computing Science and Engineering (JCSE, Kiise).

Patrick Cousot is member of the steering committees of the Static Analysis Symposium (SAS) and the Verification, Model-Checking and Abstract Interpretation (VMCAI) international conference.

— Radhia Cousot is member of the advisory board of the Higher-Order Symbolic Computation journal (HOSC, Springer) and the Central European Journal of Computer Science (CEJCS, Versita & Springer).

Radhia Cousot is member of the steering committees of the Static Analysis Symposium (SAS), the Workshop on Numerical and Symbolic Abstract Domains (NSAD), the Workshop on Static Analysis and Systems Biology (SASB) and the Workshop on Tools for Automatic Program AnalysiS (TAPAS).

Radhia Cousot was the program committee chair of the 40th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL 2013), Rome, Italy, January 23-25, 2013 [25].

Radhia Cousot was member of the program committee of the 5th NASA Formal Methods Symposium (NFM 2013), May 13-16, 2013, NASA Ames Research Center, California, USA.

— Jérôme Feret is a member of the editorial board of the Frontiers in Genetics journal and the Open Journal of Modelling and Simulation

Jérôme Feret is a member of the steering committee of the Workshop on Static Analysis and Systems Biology (SASB).

Jérôme Feret was co-program committee chair of the 4th International Workshop on Static Analysis and Systems Biology (SASB 2013), Seattle, USA, June 19, 2013.

Jérôme Feret was member of the program committees of the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013; the 5th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2013), Lisbon, Portugal, March 24-29, 2013; the 4th International Workshop on Computational Models for Cell Processes (CompMod 2013), Turku, Finland, June 11, 2013; the 11th Conference on Computational Methods in Systems Biology (CMSB 2013), Klosterneuburg, Austria, September 23-25, 2013; the 2nd International Conference on Biomedical Engineering and Biotechnology (ICBEB 2013), 2013; the 15th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2014), San Diego, USA, January 19-21, 2014. He is member of the program committees of the 6th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2014), Chamonix, France, April 20-24, 2014; the 10th International Workshop on Developments in Computational Models (DCM 2014), Vienna, Austria, July 13, 2014; the International Workshop on Verification of Molecular Devices and Programs (VEMDP 2014), Vienna, Austria, July 17, 2014; the 8th IFIP Theoretical Computer Science Conference (IFIP TCS 2014), Rome, Italy, September 1-3, 2014; the 5th International Workshop on Static Analysis and Systems Biology (SASB 2014), Munich, Germany, September 10, 2014; the 9th International Workshop on Formal Methods for Industrial Critical Systems (FMICS 2014), Florence, Italy, September 11-12, 2014; the 3rd International Conference on Biomedical Engineering and Biotechnology (ICBEB 2014), Beijing, China, September 19-21, 2014.

— Jonathan Hayman was a member of the program committees of the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013; the 4th International Workshop on Static Analysis and Systems Biology (SASB 2013), Seattle, USA, June 19, 2013.

— Antoine Miné is a member of the editorial boards of The Scientific World Journal in Computer Science and of the journal Conference Papers in Computer Science.

Antoine Miné was a member of the program committee of the 20th International Static Analysis Symposium (SAS 2013), Seattle, WA, USA, June 20–22, 2013, and the 3rd International Workshop on Safety and Security in Cyber-Physical Systems (SSCPS 2013), Washington, D.C, USA., June, 18–20, 2013. He is a member of the program committee of the 11th School on Modelling and Verifying Parallel Processes (MOVEP 2014), Nantes, France, July 7–11, 2014, the 8th International Symposium on Theoretical Aspects of Software Engineering (TASE 2014), Changsha, China, 1–3 September, 2014, the 11th International Conference on Integrated Formal Methods (iFM 2014), Bertinoro, Italy, September 9–11, 2014, and of the external review committee of the 42nd ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2015 ERC), Mumbai, India, January 11–18, 2015.

— Xavier Rival is member of the steering committee of the Workshop on Tools for Automatic Program AnalysiS (TAPAS).

Xavier Rival is Co-Chair of the program committee of the 15th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2014, San Diego, USA, January 19-21, 2014 [26].

Xavier Rival was member of the extended review committee of the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013; the program committee of the program committee the European Symposium On Programming (ESOP 2013), Rome, Italy, March 2013; the program committee of the 41st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2014), San Diego, USA, January 22-24, 2014;

9.1.4. Participation in Conferences

Luminy workshop: Workshop on Modelisation, Optimisation, and Static Analysis (Luminy, France, January 6–10, 2013).
Jérôme Feret attended the workshop and gave a talk on model reduction of Kappa models.

VMCAI: 14th International Conference on Verification, Model Checking, and Abstract Interpretation (Roma, Italy, January 20–22, 2013).
Antoine Miné, Xavier Rival, Antoine Toubhans and Caterina Urban attended the conference. Antoine Toubhans presented an article [20].

POPL: 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, (Roma, Italy, January 23–25, 2013).
Xavier Rival and Caterina Urban attended the conference.

Bytecode: Eigth Workshop on Bytecode Semantics, Verification, Analysis, and Transformation (Rome, Italy, March 23, 2013).
Mehdi Bouaziz attended the workshop and gave a talk on [11].

CC: Twenty-second International Conference on Compiler Construction (Rome, Italy, March 21–22, 2013).
Mehdi Bouaziz attended the conference.

ESOP: Twenty-second European Symposium on Programming (Rome, Italy, March 19–22, 2013).
Mehdi Bouaziz attended the conference.

FASE: Sixteenth International Conference on Fundamental Approaches to Software Engineering(Rome, Italy, March 20–22, 2013).
Mehdi Bouaziz attended the conference.

POST: Second Conference on Principles of Security and Trust (Rome, Italy, March 18–19, 2013).
Mehdi Bouaziz attended the conference.

TACAS: Nineteenth International Conference on Tools and Algorithms for the Construction and Analysis of Systems (Rome, Italy, March 18–21, 2013).
Mehdi Bouaziz attended the conference.

RBMW: Rule-Based Modelling Workshop (Paris, France, April 15–16, 2013).
Wassim Abou-jaoudé, Ferdinanda Camporesi, Jérôme Feret, and Norman Ferns attended the workshop. Jérôme Feret gave a talk on [12]. Norman Ferns gave a talk on backward bisimulation.

In'Tech: In'Tech Seminar on Formal validation of industrial critical systems (Grenoble, France, April 18, 2013).
Jérôme Feret attended the workshop and gave a talk on the ASTRÉE analyzer.

Dagstuhl 13162: Wokshop on Pointer Analysis (Dagstuhl, Germany, April 14–19, 2013).
Xavier Rival attended the workshop and gave a talk on the modular construction of shape analyzers.

SASB: Fourth International Workshop on Static Analysis and Systems Biology (Seattle, USA, June 19, 2013).
Jérôme Feret and Jonathan Hayman attended the workshop. Jérôme Feret chaired the workshop and chaired half of the sessions. Jérôme Feret gave a talk on [12] and Jonathan Hayman gave a talk on [15].

SAS: 21th International Static Analysis Symposium (Seattle, WA, USA, June 20–22, 2013).
Jérôme Feret and Caterina Urban attended the conference, and Caterina Urban presented a paper [24].

ForumMF: Deuxième Forum Méthodes Formelles, Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS-CNRS, Toulouse, France, June 28, 2013).
Mehdi Bouaziz attended the workshop and gave a talk on Specification and verification of programs with CodeContracts.

WST: 13th International Workshop on Termination (Bertinoro, Italy, 29–31 August, 2013).
Caterina Urban attended the workshop and presented an article [23].

DSS2013: Dave Schmidt Symposium (Festschrift for Dave Schmidt, Manhattan, Kansas, September 18-19, 2013).
Xavier Rival attended the symposium and presented an article [13].

In'Tech: In'Tech Seminar on Formal validation of industrial critical systems (Aix en Provence, France, October 1, 2013).
Jérôme Feret attended the workshop and gave a talk on the ASTRÉE analyzer.

CMSB: Computational Methods in Systems Biology (Klosterneuburg, Austria, September 23-25, 2013). Ferdinanda Camporesi, Jérôme Feret, and Norman Ferns attended the conference. Jérôme Feret chaired a session and gave a talk on [12].

RAIM: 6ème Rencontres Arithmétiques de l'Informatique Mathématique (Paris, France, 18–20 November, 2013).
Antoine Miné attended the conference and gave a talk on generic and specific abstract domains for the static analysis of programs with floating-point arithmetic.

AVDCPS: Workshop on Analysis and Verification of Dependable Cyber Physical Software (Changsha, November 23-24, 2013).
Mehdi Bouaziz, Tie Cheng, Jérôme Feret, Xavier Rival, and Caterina Urban attended the conference. Jérôme Feret chaired a session. Mehdi Bouaziz, Tie Cheng, Jérôme Feret, Xavier Rival, and Caterina Urban gave talks.

9.1.5. Invitations and Participation in Seminars

— Arlen Cox gave a talk at LIAFA (Paris 7) about "QUIC Graphs: Relational Invariant Generation for Containers".

— Jérôme Feret gave a talk at IRIT (Toulouse, France) on the 28th of May, 2013 about model reduction in Kappa. He gave a talk on the OpenKappa platform at a meeting of the ANR BIOTEMPO project on the 30th of January, 2013 and a talk on context sensitive model reduction [12] at another meeting of the ANR BIOTEMPO project in Paris on the 10th of April, 2013. He gave a talk on context sensitive model reduction [12] at ETH Zürich on the 5th of June, 2013. He gave on talk on the analysis of digital filters [55], [56] at a meeting of the ANR VERASCO on the 16th of September, 2013.

— Norman Ferns gave two talks on the Kantorovich metric at the Computer Science Seminar of the University of Liège, Belgium, on the 5th of April 2013 and at the Technical Talk Seminar of the TU Dortmund University, Germany, on the 5th of July 2013.

— Antoine Miné gave a talk on "Constraint solving using numeric abstract domains" at the LIAFA Seminar "Vérification" (Paris, France) on April the 8th, 2013 and at the CEA LSL/LMeasi Seminar (Palaiseau, France) on June the 4th, 2013.

— Caterina Urban gave a talk on "The abstract domain of segmented ranking functions" at University of Udine (Italy) in March 2013.

— Xavier Rival gave a talk on the combination of memory abstractions at the IFIP 2.4 Working Group (Mysore, India, March 2013). He gave a talk on hierarchical shape abstract domains at IBM (Bangalore, India, March 2013). He gave a talk on the modular construction of shape analyzers at LIAFA (Université Paris 7, May 2013), at Cambridge University (Cambridge, UK, September 2013), at Seoul National University (Seoul, South Korea, October 2013), at KAIST (Daejon, South Korea, November 2013), at Hanyang University (Ansan, South Korea, November 2013), at the Institute of Software of the Chinese Accademy of Sciences (Beijing, November 2013). He gave a talk on the static analysis of safety critical embedded systems at Seoul National University (Seoul, South Korea, October 2013) and at KAIST (Daejon, South Korea, November 2013). He gave a talk on hierarchical shape abstract domains at Seoul National University (Seoul, South Korea, November 2013).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence :

- Medhi Bouaziz, Introduction to Programmation and Computer Sciences (Practical Works), 36ETD, L1, Université Paris-Diderot, France.
- Mehdi Bouaziz, Intensive course of algorithm, 35h ETD, Epita, Le Kremlin-Bicêtre, France.

- Mehdi Bouaziz, Preparation to the International Olympiad in Informatics, 40h ETD, Epita, Le Kremlin-Bicètre, France.
- Mehdi Bouaziz took the French team to the International Olympiad in Informatics at Brisbane, Australia.
- Tie Cheng, Introduction to algorithmics, 42h ETD, L3, École Polytechnique, Palaiseau, France.
- Jérôme Feret, and Caterina Urban, Mathematics, 40h ETD, L1, Licence Frontiers in Life Sciences (FdV), Université Paris-Descartes, France.
- Xavier Rival, Introduction to algorithmics, 40h ETD, L3, École Polytechnique, Palaiseau, France.
- Arnaud Spiwack, Introduction to recursive programming, 42h ETD, Université Pierre et Marie Curie (Paris 6), Paris, France.
- Antoine Toubans, Mathematics, 40hETD, L2, Université de Jussieu, Paris, France.

Master :

- Jérôme Feret, Computational Biology, 9h ETD, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.
- Jérôme Feret, Antoine Miné, and Xavier Rival, Abstract Interpretation: application to verification and static analysis, 72h ETD, M2. Parisian Master of Research in Computer Science (MPRI). École normale supérieure. France.
- Xavier Rival, 20h ETD, M1, École Polytechnique, Palaiseau, France.
- Mehdi Bouaziz, Tie Cheng, Jérôme Feret, Antoine Miné, Xavier Rival, Caterina Urban, Abstract Interpretation, 30h ETD, M1-M2. East China Normal University, Shanghai, China.

Doctorat :

- Jérôme Feret, Abstract interpretation of intracellular signaling pathways, 4.5h ETD, CNRS Summer School on Formal modeling of Biological Regulatory Networks, Porquerolles, France.
- Antoine Miné, Inferring affine program invariants by abstract interpretation, 4.5h ETD, Spring School on Polyhedra Code Analysis and Optimization, Saint Germain au Mont d'Or, France, May 13–17, 2013.

9.2.2. Supervision

HdR : Antoine Miné, Static analysis by abstract interpretation of concurrent programs, École normale supérieure, 28 May 2013.

PhD in progress:

- Mehdi Bouaziz, Static analysis of security properties by abstract interpretation. November 2011, Patrick Cousot and Jérôme Feret, École Normale Supérieure.
- Ferdinanda Camporesi, Abstraction of Quantitative Semantics of Rule-based models, January 2009, Radhia Cousot and Jérôme Feret (co-directed thesis with Maurizio Gabrielli, University of Bologna).
- Arlen Cox, Representing dynamic languages heaps using parametric, modular, container abstract domains, 2013, Xavier Rival, École Normale Supérieure (co-directed thesis with Bor-Yuh Evan Chang, University of Colorado at Boulder).
- Tie Cheng, Static analysis of spreadsheet macros, October 2011, Xavier Rival, École Polytechnique.
- Vincent Laviron, Static Analysis of Functional Programs by Abstract Interpretation, October 2009, Patrick Cousot, École Normale Supérieure.

- Jiangchao Liu, Verification of the memory safety of a micro-kernel, December 2013, Xavier Rival, École Normale Supérieure
- Antoine Toubhans, Combination of shape abstract domains, October 2011, Xavier Rival, École Doctorale de Paris Centre
- Caterina Urban, Static Analysis of Functional Temporal Properties of Programs by Abstract Interpretation, November 2011, Radhia Cousot and Antoine Miné, École Normale Supérieure.

9.2.3. Juries

— Jérôme Feret reviewed the PhD thesis of Tatjana Petrov (ETH Zürich, Switzerland, JUne 6, 2013). He was also in the jury of Geoffroy Andrieux PhD thesis (Université Rennes 1, France, July 18, 2013).

— Antoine Miné reviewed the PhD thesis of Yassamine Seladji (CEA, Palaiseau, France, October 31, 2013). He was also in the jury of the PhD theses of Ramakrishna Upadrasta (Université Paris Sud, March 13, 2013) and Zhoulai Fu (Université Rennes 1, July 22, 2013).

— Xavier Rival reviewed the PhD theses of Valentin Perelle (Verimag, Université Joseph Fourrier, Grenoble, February 22, 2013) and of Gideon Smeding (Inria Rhône-Alpes, Université Joseph Fourrier, Grenoble, December 19, 2013).

9.3. Popularization

Xavier Rival gave an interview about the verification of safety critical embedded softwares to the “Inriality” online magazine, in July 2013.

CELTIQUE Project-Team

8. Dissemination

8.1. Scientific Animation

Sandrine Blazy and David Pichardie co-chaired and organized in Rennes the international conference ITP 2013 and its 2 related workshops. Sandrine Blazy is a member of the steering committee of the ITP conference. Sandrine Blazy served on the organizing committee of the international conferences VMCAI 2013 and LPAR 2013. Sandrine Blazy was scientific director of the "Languages and software engineering department" of IRISA until September 2013. Sandrine Blazy gave an invited talk at the VSTTE 2013 conference in Menlo Park, USA. David Pichardie served on the external reviewing committee of the international conference PLDI 2013 and the organizing committee of the international workshops BYTECODE 2013, PxTP 2013 and Coq Workshop 2013. David Pichardie is chair of the department of Computer Science at ENS Rennes. Alan Schmitt co-chaired and organized the International Symposium on Database Programming Languages, co-located with VLDB, in Trento, Italy (http://dbpl2013.inria.fr/). He also participated in the organization of the Programming Languages Mentoring Workshop, co-located with POPL, in Roma, Italy (http://www.doc.ic.ac.uk/~gds/PLMW/index.html). Alan Schmitt is a member of the steering committee of the Journées Francophones des Langages Applicatifs. Thomas Jensen and Alan Schmitt organized the École Jeunes Chercheurs en Programmation (EJCP 2013).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Frédéric Besson, Compilation, 68h, level M1, Insa Rennes, France

Licence : Sandrine Blazy, Programmation fonctionnelle, 30h, L3, Rennes 1, France

Master : Sandrine Blazy, Méthodes Formelles pour le développement de logiciels sûrs, 53h, M1, Rennes 1, France

Master : Sandrine Blazy, Software vulnerabilities, 26h, M2, Rennes 1

Master : Sandrine Blazy, Mechanised semantics, 15h, M2, Rennes 1, France

Licence : David Cachera, Formal Languages and Computability, 24h, L3, ENS Rennes

Licence : David Cachera, Logics, 24h, L3, ENS Rennes

Licence : David Cachera, Algorithmics, 12h, L3, ENS Rennes

Master : David Cachera, Programming Language Semantics, 24h, M1, Rennes 1

Licence : Delphine Demange, Algorithmique et Programmation Fonctionnelle, 80h, level L1, Université de Rennes 1 / Istic, France

Master : Delphine Demange, Sémantique, 8h, level M1, Université de Rennes 1 / Istic / ENS Cachan Antenne Bretagne, France

Licence : Thomas Genet, Programmation fonctionnelle, 32h, niveau L3, Université de Rennes 1 / Istic, France

Master : Thomas Genet, Conception et vérification formelle, 90h, niveau M1, Université de Rennes 1 / Istic, France

Master : Thomas Genet, Protocoles cryptographiques, 24h, niveau M2, Université de Rennes 1 / Istic, France

Master : Thomas Jensen, Program analysis, 14h, M2, Rennes

Master : Thomas Jensen, Software security, 20h, M2, Rennes

Licence : David Pichardie, Algorithms, 60h, L3, ENS Rennes

Master : David Pichardie, Mechanised semantics, 15h, M2, Rennes 1, France

Master : David Pichardie, Program analysis, 6h, M2, Rennes

Licence : Alan Schmitt, Programmation Fonctionnelle, 37h, niveau L3, Insa Rennes, France

8.2.2. Supervision

PhD : Pierre-Emmanuel Cornilleau, Certification of static analysis in many-sorted first-order logic, ENS Cachan - antenne de bretagne, 25 march 2013, Thomas Jensen and Frédéric Besson

PhD in progress : Pierre Wilke, Retro-engineering of auto-modifying code by static analysis, 1st august 2013, Sandrine Blazy and Frédéric Besson

PhD in progress : Valérie Murat, Automatic Verification of infinite state systems by tree automata completion, 1st august 2011, Thomas Genet

PhD in progress : Yann Salmon, Reachability for Term Rewriting Systems under Strategies, 1st august 2012, Thomas Genet

PhD in progress: Andre Oliveira Maroneze, Compilation vérifiée et calcul de temps d'exécution au pire cas, septembre 2010, Sandrine Blazy, David Pichardie and Isabelle Puaut

PhD in progress: Stéphanie Riaud, Transformations de programmes pertinentes pour la sécurité du logiciel, septembre 2011, Sandrine Blazy

PhD in progress: Vincent Laporte, Formal verification of static analyses for low level langages, septembre 2012, Sandrine Blazy and David Pichardie

PhD in progress: David Bühler, Communication between analyses by deductive verification and abstract interpretation, November 2013, Sandrine Blazy and Boris Yakobowski (CEA)

PhD in progress : Martin Bodin, Certified Analyses of JavaScript, 1st september 2012, Thomas Jensen and Alan Schmitt

PhD in progress : Oana Andreescu, Proof reusability in the formal modeling of secure operating systems, 1st September 2013, Thomas Jensen and Stephane Lescuyer (Prove & Run)

PhD in progress : Pauline Bolignano, Formal methods for minimizing a trusted computing base in an operating system, 1st October 2013, Thomas Jensen and Vincent Siles (Prove & Run)

8.2.3. Juries

Frédéric Besson, jury member for the PhD defense of Mohamed Iguernelala, July 10th 2013

Sandrine Blazy, jury member (reviewer) for the PhD defense of Cédric Auger, February 2013, University Paris Sud

Sandrine Blazy, jury member (reviewer) for the PhD defense of Suman Saha, March 2013, University Paris 6

Sandrine Blazy, jury member (president) for the PhD defense of Benjamin Lesage, May 2013, University Rennes 1

Sandrine Blazy, jury member (reviewer) for the PhD defense of Xiaomu Shi, July 2013, Grenoble University

Sandrine Blazy, jury member for the PhD defense of Pierre Néron, October 2013, École Polytechnique

Sandrine Blazy, jury member (reviewer) for the PhD defense of Jean Fortin, October 2013, University Paris East

Thomas Jensen, jury member (examiner) for the PhD defense of Andreas lundblad, March 2013, Royal Technological University, Stockholm, Sweden.

Thomas Jensen, jury member (reviewer) for the PhD defense of Michal Terepeta, October 2013, Technical University, Denmark.

Thomas Jensen, jury member (president) for the PhD defense of Yassamine Seladji, November 2013, Ecole Polytechnique.

Thomas Jensen, jury member (reviewer,president) for the PhD defense of Quentin Sabah, December 2013, University of Grenoble.

David Pichardie, jury member (president) for the PhD defense of Sebastien Chédor, December 2013, University Rennes 1

8.3. Popularization

Frédéric Besson and Nataliia Bielova have presented their approach for quantifying web-fingerprinting in the "Du côté de la recherche" section of the November issue of Ouest Inria.

David Pichardie organised the third edition of the french Castor Informatique contest. This contest promotes Computer Science in secondary schools and high schools. It is organised by Inria, ENS Cachan and the France IOI association and supported by CNRS, Pascaline, the SIF and API associations. In 2013, there was about 170.000 participants.

DEDUCTEAM Exploratory Action

8. Dissemination

8.1. Scientific Animation

- Guillaume Burel has been a PC member of IWIL.
- David Delahaye has been a PC member of PxTP 2013. He is a member of the steering committee of Calculemus since 2010.
- Gilles Dowek has been a PC member of RTA, ICECCS, NFM and eMooc.
- Gilles Dowek is a member of the Cerna.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Bachelor: Ali Assaf, Les bases de la programmation et de l'algorithmique, 36 hours, third year, École Polytechnique, France

Bachelor: Ali Assaf, Algorithmique et programmation, 36 hours, third year, École Polytechnique, France

Bachelor: Alejandro Díaz-Caro, Mathématiques 1: Calcul et fonctions, 72 hours, 1st year, Université Paris X, France

Bachelor: Alejandro Díaz-Caro, Statistiques et probabilités, 6 hours, second year, Université Paris X, France

Bachelor: Alejandro Díaz-Caro, Mathématiques 2, 24 hours, first year, Université Paris X, France

Bachelor: Alejandro Díaz-Caro, Méthodologie de la mesure en sciences humaines, 48 hours, first year, Université Paris X, France

Bachelor: Ronan Saillard, Programmation Orientée Objet en Java, 27 hours ,Telecom ParisTech, France

Bachelor: Guillaume Burel, Programmation avancée, 25,5 hours, third year, ENSIIE, France

Bachelor: Guillaume Burel, Logique, 10,5 hours, third year, ENSIIE, France

Bachelor: Guillaume Burel, Projet informatique, 22,75 hours, third year, ENSIIE, France

Master: Guillaume Burel, Systèmes et langages formels, 21 hours, first year, ENSIIE, France

Master: Guillaume Burel, Compilation, 36,75 hours, first year, ENSIIE, France

Master: Guillaume Burel, Sémantique des langages de programmation, 21hours, second year, ENSIIE, France

Master: Pierre Halmagrand, Sureté fonctionnelle, 12,5 hours, second year, CNAM Saint-Denis, France

Master: Olivier Hermant, Méthodes formelles, 21 hours, second year, ISEP, France

Master: Olivier Hermant, Algorithmique, 9 hours, second year, ISEP, France

Master: Olivier Hermant, Complétude et élimination des coupures, 1,5 hours, second year, Université Paris Diderot, France

Master: Gilles Dowek, Fondement des systèmes de preuves, 27 hours, second year, MPRI.

Guillaume Burel is in charge of the 4th, 5th, and 6th semesters of the engineering degree at ENSIIE.

David Delahaye has taught at *Cnam* courses in the following topics: Algorithmics, Object-Oriented Programming Languages, Safety and Security, Formal Proofs and Automated Deduction.

8.2.2. Supervision

PhD in progress : Ali Assaf, Interoperabilty of proof systems, September 2012, Gilles Dowek and Guillaume Burel

PhD in progress: Raphaël Cauderlier, Mécanismes orientés objets pour le raffinement de données et d'algorithmes dans les systèmes de preuve, September 2013, Catherine Dubois

PhD in progress : Simon Cruanes, Automated reasoning modulo theories, August 2012, Gilles Dowek and Guillaume Burel

PhD in progress : Kailiang Ji, Model checking and automated theorem proving, September 2012, Gilles Dowek

PhD in progress: Kim-Quyen Ly, automated formal verification of termination certificates, October 2011, Frédéric Blanqui

PhD in progress: Pierre Halmagrand, Déduction automatique modulo, November 2013, David Delahaye and Olivier Hermant and Damien Doligez

PhD in progress: Vivien Maisonneuve, Préservation de preuve de système lors de la compilation sur micro-contrôleur, October 2011, François Irigoin and Olivier Hermant

PhD: Pierre Néron: A Quest for Exactness: Program Transformation for Reliable Real Numbers, December 2013, Gilles Dowek.

PhD in progress: Ronan Saillard, Dedukti: un vérificateur de preuves universel, October 2012, Pierre Jouvelot and Olivier Hermant

- David Delahaye, Olivier Hermant, and Damien Doligez have supervised the Master internship of Pierre Halmagrand.
- Catherine Dubois has supervised the undergrad internship of Frédéric Lang.

8.2.3. PhD and Habilitation juries

- Catherine Dubois has been a member of the PhD juries of Mounira Kezadri and Asma Tafat.
- Gilles Dowek has been a member of the Phd juries of Jianhua Gao, Maël Pégny, Alberto Naibo, and to the HDR jury of Benjamin Nguyen.

8.3. Popularization

- **Seminars in international workshops without peer review**
  - Alejandro Díaz-Caro. Identifying isomorphic propositions. In *First Workshop of ANR-NSFC project LOCALI*. Beijing, China. November 4–6.
  - Pierre Halmagrand. Proof compression and certification in Zenon Modulo. In *Third Workshop of the Amadeus Project for Proof Compression*. Nancy, France. September 16.
  - Gilles Dowek has participated to the workshop Locali in Beijing where he has given a talk.
- **Seminars in national workshops without peer review**
  - Alejandro Díaz-Caro. Identifying isomorphic propositions. In *Journées LAC*. Créteil, France. November 28–29.
  - Alejandro Díaz-Caro. Vectorial types, non-determinism and probabilistic systems: Towards a computational quantum logic. In *Quantum Computing in Nancy*. Nancy, France. March 21.
  - Gilles Dowek has participated to the workshop Rochebrune 2013 *La preuve et ses moyens*, where he has given a talk.
  - Gilles Dowek has given several talks on Computer Science in Education, at the congrès de la SIF, the workshop EPI in Nancy, the workshop UPS in Luminy, the journée ISN in Orsay, the journée Pascaline in Paris, etc.

  - Gilles Dowek has given several popular science talks: in Paris for the young kangaroos, in Athens, and in the Lycée Raoul Folleraux.

- **Other seminars**
  - Alejandro Díaz-Caro. Hacia una lógica computacional cuántica. FCEIA, Universidad Nacional de Rosario. Rosario, Argentine. August 9.
  - Alejandro Díaz-Caro. Vectorial types, non-determinism and probabilistic systems: Towards a quantum computational logic. PPS, Université Paris-Diderot. Paris, France. May 7.
  - Alejandro Díaz-Caro. Vectorial types, non-determinism and probabilistic systems: Towards a quantum computational logic. LIAFA, Université Paris-Diderot. Paris, France. April 16.
  - Alejandro Díaz-Caro. Non determinism (and probabilities) through type isomorphism. LIP, École Normale Supérieure. Lyon, France. February 21.
  - Alejandro Díaz-Caro. Quantum computing, non-determinism, probabilistic systems...and the logic behind. Modal'X. Université Paris X. Nanterre, France. January 31.
  - Pierre Halmagrand. Zenon Modulo: When Achilles outruns the tortoise using Deduction modulo. Mines ParisTech laboratory CRI. Fontainebleau, France. October 30.

GALLIUM Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Conference organization

Didier Rémy organized the October 2013 meeting of IFIP working group 2.8 “Functional programming”, which took place in Aussois, France.

Thomas Braibant participated in the organization of the LOLA 2013 workshop, associated with LICS 2013.

9.1.2. Editorial boards

Xavier Leroy is on the editorial board for the Research Highlights column of Communications of the ACM. He is a member of the editorial boards of Journal of Automated Reasoning, Journal of Functional Programming, and Journal of Formalized Reasoning.

9.1.3. Program committees

Xavier Leroy was a member of the program committee for VSTTE 2013, the conference on Verified Software: Theory, Tools and Experiments.

François Pottier was a member of the program committee for ESOP 2014, the European Symposium On Programming.

9.1.4. Steering committees

Xavier Leroy is a member of the steering committees for the Certified Programming and Proofs (CPP) conference and the Programming Languages meet Program Verification (PLPV) workshop.

François Pottier is a member of the steering committee for the ACM TLDI workshop.

Didier Rémy is a member of the steering committee of the OCaml Workshop.

9.1.5. Collective responsibilities

Damien Doligez chairs the *Commission des actions de développement technologiques* of Inria Paris-Rocquencourt.

Xavier Leroy is *vice-président du comité des projets* of Inria Paris-Rocquencourt and appointed member of *Commission d'Évaluation*. He participated in the following Inria hiring and promotion committees: *jury d'admissibilité CR2 Paris-Rocquencourt* (vice-chair, with Philippe Robert as chair); *jury d'admissibilité DR2*; *promotions CR1, DR1, DR0*. He was a member of the hiring committee for a *Maître de conférences* position at Université Rennes 1.

Luc Maranget chairs the *Commission des utilisateurs des moyens informatiques – Recherche* of Inria Paris-Rocquencourt.

François Pottier is a member of the post-doctoral hiring committee of Inria Paris-Rocquencourt. He was a member of the hiring committee for a *Maître de conférences* position at Université Paris Diderot.

Jonathan Protzenko curated the Junior Seminar of Inria Paris-Rocquencourt until June 2013, which marked the end of his two-year involvement in the seminar.

Didier Rémy represents Inria in the *commission des études* of the MPRI master, co-organized by U. Paris Diderot, ENS Cachan, ENS Paris, and École Polytechnique.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Thibaut Balabonski, “Travaux dirigés de Caml Light”, 14 hours, L1, Collège Stanislas (classes préparatoires MPSI), France.

Licence: Julien Cretin, “Bases de données”, 26h, L3, U. Paris Diderot, France.

Licence: Julien Cretin, “Principe de fonctionnement des machines binaires”, 33h, L1, U. Paris Diderot, France.

Licence: Jacques-Henri Jourdan, “Langages de programmation et compilation”, 46h, L3, École Normale Supérieure, France.

Licence: François Pottier, “Algorithmique et programmation” (INF431), 13h30, L3, École Polytechnique, France.

Licence: Gabriel Scherer, “IF1: Introduction to computer science and programming”, 42h, L1, U. Paris Diderot, France.

Master: Xavier Leroy and Didier Rémy, “Functional programming and type systems”, 12h + 18h, M2, MPRI master, France.

Master: Luc Maranget, “Semantics, languages and algorithms for multicore programming”, 9h, M2, MPRI master, France.

Master: François Pottier, “Compilation” (INF564), 13h30, M1, École Polytechnique, France.

Master: Jonathan Protzenko, “Conception et mise en œuvre d’algorithmes” (MOOC), 32h, M1, Coursera / École Polytechnique, France.

Master: Gabriel Scherer, “Advanced Functional Programming”, 30h, M1, U. Paris Diderot, France.

Doctorat: Xavier Leroy, “Mechanized semantics”, 6h, Verification Technology, Systems & Applications summer school 2013, Nancy, France.

9.2.2. Supervision

PhD in progress: Julien Cretin, “Erasable coercions: a unified approach to type systems”, École Polytechnique, since December 2010, supervised by Didier Rémy, to be defended January 30th, 2014.

PhD in progress: Pierre Halmagrand, “Déduction Automatique Modulo”, CNAM, since September 2013, supervised by David Delahaye, Damien Doligez, and Olivier Hermant.

PhD in progress: Jonathan Protzenko, “Fine-grained static control of side effects”, U. Paris Diderot, since September 2010, supervised by François Pottier.

PhD in progress: Gabriel Scherer, “Term inference”, U. Paris Diderot, since October 2011, supervised by Didier Rémy.

PhD in progress: Jacques-Henri Jourdan, “Formal verification of a static analyzer for critical embedded software”, U. Paris Diderot, since September 2012, supervised by Xavier Leroy.

9.2.3. Juries

Damien Doligez was a member of the Ph.D. jury of Mélanie Jacquel, CNAM, Paris, april 2013.

Xavier Leroy was a member of the Ph.D. jury of Xiaomu Shi, Université Joseph Fourier, Grenoble, july 2013.
Xavier Leroy was president of the Ph.D. jury of Pierre-Nicolas Tollitte, CNAM, Paris, december 2013.

9.3. Popularization

Jacques-Henri Jourdan and Arthur Charguéraud participated in the organization of the Castor computer science contest (http://castor-informatique.fr/). This contest aims at making computer science more popular in French high schools and junior high schools. It attracted over 170,000 participants.

Fabrice Le Fessant is one of the organizers of the OCaml meetup in Paris. Four events were organized in 2013, each featuring four short presentations on topics related to OCaml. Each event was attended by about 60 participants.

Xavier Leroy gave a tutorial on using theorem provers in programming language research at the 2013 ACM SIGPLAN Programming Languages Mentoring Workshop, which was attended by about 80 undergraduate, graduate and post-doctoral students.

Since 2012, the Gallium team publishes a research blog at http://gallium.inria.fr/blog/, edited by Gabriel Scherer. This blog continued its activity in 2013, with 26 posts by 12 different authors. It covered various changes in the OCaml language, announced small software libraries from members of the team, and discussed Gallium's research, notably the Mezzo language.

MARELLE Project-Team

8. Dissemination

8.1. Scientific Animation

Members of the project refereed papers for the journals MSCS (Mathematical Structures of Computer Science), JFR (Journal of Formalized Reasoning), they participated to the program committee of ITP (Interactive Theorem Provers),ACL2 (A Computational Logic for Applicative Common Lisp), PxTP (Proof Exchange for Theorem Provers), and refereed papers for the conferences ITP and ESOP (European Symposium on Programming),ISSAC (International Symposium on Symbolic and Algebraic Computation).

Benjamin Grégoire gave lectures at the first EasyCrypt summer school in Philadelphia in July.

Members of the project participated to the conferences "Journées Francophones des Langages Applicatifs" (Aussois, France, January) "workshop on Foundation of Mathematics for Computer-Aided Formalization" (Padova, Italy, January), "Journées Nationales de l'Informatique Mathématique" (Lyon, January),"Conferences on Inteligent Computer Mathematics" (London, July), "Conference on Interactive Theorem Proving" (Rennes, France), "Conference on Symbolic and Numerical Algorithms for Scientific Computing" (Timisoara, Romania, September).

Yves Bertot was invited to give a joint seminar on homotopy type theory at Harvard in Boston, USA, and MIT on March 25th, 2013, Benjamin Grégoire made 8 visits to IMDEA in Madrid, Spain, to work on formally verified proofs in cryptography and automatic tools for formal verification for cryptographers, L. Rideau, L. Théry, E. Martin-Dorel were invited to meetings in Lyon, in July and October, Y. Bertot, L. Rideau participated to the Spring Day of Microsoft Research-Inria joint centre.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Laurence Rideau, "Introduction to programming" classe préparatoire MP*, teaching assistant, 48 hours, Lycée Masséna, Nice, France

Master : Laurent Théry: "Formalization of floating point arithmetic", 8 hours, ENS Lyon, France

Master : Laurent Théry: "Introduction to Coq", 3 hours, École des Mines de Paris, Sophia Antipolis, France

Master : Laurent Théry: Examiner for the exam "agrégation de mathématiques, option informatique"

Master : Julianna Zsidó: "Logic", 48 hours, École Polytechnique Universitaire, Sophia Antipolis, France

8.2.2. Supervision

PhD : Maxime Dénès, "Étude formelle d'algorithmes efficaces en algèbre linéaire", Université de Nice, defended on November, 20th, 2013, supervised by Yves Bertot.

PhD in progress: Maxime Cano, "Interaction entre algèbre linéaire et analyse en formalisation des mathématiques", thèse commencée en octobre 2010, supervised par Yves Bertot.

8.2.3. Juries

- Yves Bertot was an examiner for the thesis defense of Shi Xiaomu (University of Grenoble, France and Tsinghua University, Beijing, China), María Poza (Universidad de la Rioja, Spain–with written report duty), Pierre Néron (Ecole Polytechnique, France–as chairman for the Jury), Victor Magron (Ecole Polytechnique, France–with written report duty).

- Benjamin Grégoire was an examiner for the thesis of Chantal Keller (Ecole Polytechnique, France).

8.2.4. Community Service

- José Grimm is a member of the *comité de centre*, the committee where representatives of personnel and management discuss questions of daily life at the level of the Sophia-Antipolis Méditerranée center, he also participates in a commision on continued training and a commission on hygiene, safety, and working conditions. This activity involves around 12 meetings per year.
- Benjamin Grégoire was a member of the *comité de développement technologique* (in English, technological development committee), the committe that overseas the allocation of software engineers on experimental software and platform development, until June 2013. Laurent Théry is a member of the same committee since June 2013.
- Benjamin Grégoire and Yves Bertot are members of the Coq steering committee. Yves Bertot has been appointed chairman of this committee since October 2013. As such, Yves Bertot attended a Coq users meeting at ICFP in 2013.
- Yves Bertot is deputy scientific director for the Sophia Antipolis méditerranée research center. This task implies meetings approximately every fortnight with the center director, the scientific director, and the director of admnistrative services for the center, together with frequent meetings with researchers from any domain in the center and monthly meetings at the national level as part of the evaluation committee.

8.3. Popularization

Yves Bertot participated to two articles published in popular science magazines (*Science et Vie* and *Science et Avenir*) and Laurence Rideau to one of these articles.

MEXICO Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Benedikt Bollig

was on the program committee of *YR-CONCUR 2013*. He also was a member of the commission scientifique Inria Saclay.

8.1.2. Thomas Chatain

was on the program committee *ACSD 2013* and of *FORMATS 2013*. He also participated in the organization of the latter.

8.1.3. Paul Gastin

is co-head (with Madhavan Mukund) of the new International Associated Laboratory (LIA) INFORMEL (INdo-French FORmal Methods Lab). This LIA was created in January 2012 by an agreement between CNRS, ENS Cachan, University Bordeaux 1 on the french side and the Chennai Mathematical Institute, the Institute of Mathematical Sciences of Chennai, and the Indian Institute of Science of Bangalore on the Indian side.

He is the head of the computer science department of ENS Cachan.

Paul Gastin is an associate editor of the Journal of Automata, Languages and Combinatorics.

He is on the Advisory Board of the EATCS-Springer book series

- Monographs in Theoretical Computer Science,
- Texts in Theoretical Computer Science.

8.1.4. Stefan Haar

is an associated editor for the journal *Discrete Event Dynamic Systems: Theory and Application*, and was on the program committee of *PNSE 2013*. At the Inria Center Saclay, Stefan was the correspondent for international relations until September 2013 (his successor is Benjamin Smith), and has since become the correspondent for European Partnerships; he continues as a member of the GTRI (working group on international relations) of Inria's *COST*. In 2013 he also joined the DIGITEO program committee.

8.1.5. Serge Haddad

has been a member of the steering committee of the international conference Applications and Theory of Petri Nets (ATPN) since 2001. In 2013, he was a member of the following program committees of international conferences:

- *7th International Workshop on Verification and Evaluation of Computer and Communication systems*, Florence, Italy;
- *21st International Conference on Real Time Networks and Systems (RTNS 2013)*, Sophia-Antipolis, France;
- PC Co-Chaire of *SMC*, associated workshop at *Run-Time Verification 2013*, Rennes, France;
- *33rd International Conference on Application and Theory of Petri Nets (ATPN)*, Milan, Italy;
- *Petri Nets in Software Engineering (PNSE)*, associated Workshop at ATPN 2013.

Serge Haddad served on the program committees of the following national conferences:

- *9ème Colloque Francophone sur la Modélisation des Systèmes Réactifs (MSR) 2013*, Rennes
- *Ecole d'été Temps Réel (ETR) 2013*, Toulouse.

8.1.6. Claudine Picaronny

is a member of the Program committee of the *SIMUL* conference. She is a *Maître de Conférence* at ENS Cachan, and in charge of the Master M2 FESUP and the *préparation à l'agrégation en mathématiques* at ENSC. Moreover, Claudine Picaronny is a member of the jury for the second ENSC entrance examination in mathematics, coordinator of the entrance examinations MP and PC of the groupe E3A, and of the jury of the national olympics in mathematics and computer science.

8.1.7. Stefan Schwoon

was on the program committee of *SPIN 2013*.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Here we present the teaching activities of *researchers*; note that in addition to the classes here, five team members (Th. Chatain, P. Gastin, S. Haddad, C. Picaronny and S. Schwoon) are full-time professors (*professeurs* ou *maître de conférences*) of ENS Cachan and fulfill their teaching obligations there.

Master : Stefan Haar, *Analyse structurelle de Réseaux de Petri*, 15 TDEQ, M2 SAR, UPMC

Agrégation: Stefan Haar, Algorithmique, ca. 20 TDEQ, *Préparation Agrégation option informatiqe*, ENS Cachan

Thomas Chatain and Stefan Schwoon gave lectures on unfoldings of Petri nets at the Petri Nets 2013 conference.

8.2.2. Supervision

8.2.2.1. HdR

Thomas Chatain, *Concurrency in Real-Time Distributed Systems, from Unfoldings to Implementability*, ENS Cachan, defended Dec. 13, 2013; *garant*: Stefan Haar

HdR : Stefan Schwoon, *Efficient verification of sequential and concurrent systems*, ENS Cachan, defended Dec. 6, 2013; *garant*: Stefan Haar

8.2.2.2. PhD

Benjamin Monmege, *Specification and Verification of Quantitative Properties: Expressions, Logics, and Automata* , ENS Cachan, defended Oct 24, 2013; Supervisors: Paul Gastin and Benedikt Bollig.

César Rodrîguez, *Verification Based on Unfoldings of Petri Nets with Read Arcs*, ENS Cachan, defended Dec 12, 2013; Supervisor: Stefan Schwoon

8.2.2.3. PhD in progress

Benoît Barbot, *Rare event handling in statistical model checking*, since September 2011; Supervisors: Serge Haddad and Claudine Picaronny.

Aiswarya Cyriac, *Verification of Communicating Recursive Programs via Split-width*, since September 2010; Supervisors: Paul Gastin and Benedikt Bollig.

Hernán Ponce de Léon, Testing concurrent systems using event structures, ENS Cachan, since September 2011; Supervisors: Stefan Haar and Delphine Longuet

Simon Theissing, Supervision of Multi-Modal Transport Systems, since September 2013, ENS Cachan/Inria/IRT SystemX project MIC; Supervisor: Stefan Haar

Salim Perchy, *D-Spaces*, Ecole Polytechnique, since November 2013; main supervisor : Supervisors: Frank D. Valencia (COMETE Team) and Stefan Haar

8.2.3. Juries

8.2.3.1. Paul Gastin

was a reviewer

- of the PhD thesis of Amélie Stainer, Rennes , defended on Nov. 25;
- and of the HdR thesis of Loic Helouet, Rennes, defended on May 17.

As supervisor of Benjamin Monmege, he also served as *rapporteur* on the jury of his defense, on Oct 24.

8.2.3.2. Stefan Haar

was a reviewer of the PhD theses of

- Elisabeta Mangioni, Univ. Milan-Bicocca, Italy,
- Florent Avellaneda, Univ. Aix-Marseille, defended Dec 10, and
- Sébastien Chédor, Université Rennes 1, defended on January 7, 2014.

Except for the defence of E. Mangioni, he also participated in the respective juries. Moreover, he was jury president for the defence of Aurore Junier, ENS Cachan, defended on December 16 in Rennes, and *examinateur* in the PhD jury of César Rodríguez, defended December 12. He also was a member of the HdR juries (as *garant*) of Stefan Schwoon (December 6) and Thomas Chatain (December 13), both at ENS Cachan.

8.2.3.3. Serge Haddad

was a reviewer for the PhD thesis of Henri Debrat in Nancy and member of the Jury on December 6, 2013. He also served on the jury for the HdR of Kais Klai at Université Paris 13/ Nord on December 9, 2013.

8.2.3.4. Stefan Schwoon

was *examinateur* for the PhD thesis of Yan Zhang at Université Paris 6. [18], [22], [23], [17], [19], [21]

8.3. Popularization

Benedikt Bollig gave an invited talk at the German Workshop “Automaten und Logik”, held on September 25, 2013, in Ilmenau.

Paul Gastin has given a talk on *"Automates: Applications et Algorithmique"* during the *Rencontres Algorithmiques et Programmation*, addressing secondary teachers of the *classes préparatoires* level, at CIRM Marseille, 6 to 10 May. He also gave an invited talk on *Evaluation of Weighted Specifications over Nested Words* for the opening of the research training group *Quantitative Logics and Automata (QuantLa)*, Leipzig, on April 30.

PARSIFAL Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Organization

Dale Miller served on the Program Committee of Tableaux 2013, 16-19 September, Nancy, France.

Dale Miller is the editor-in-chief of the ACM Transactions on Computational Logic (ToCL) (June 2009 - May 2015).

Dale Miller has editorial duties on the following three other journals: *Journal of Automated Reasoning*, published by Springer (member of Editorial Board since 2011), *Theory and Practice of Logic Programming* published by Cambridge University Press (an editorial advisor since 1999), and *Journal of Applied Logic*, published by Elsevier (an area editor for "Type Theory for Theorem Proving Systems" since 2003).

Dale Miller is a member of the selection jury for the 2013 E. W. Beth Dissertation Award of the Association for Logic, Language and Information.

8.1.2. Invited Talks

François Lamarche gave a total of eight hours of lectures on path functors at the Groupe de Travail sur les Catégories supérieures, polygraphes et homotopie at the PPS laboratory, Université Paris VII.

Dale Miller gave an invited talk at LFMTP 2013: Logical Frameworks and Meta-Languages: Theory and Practice, affiliated with ICFP'13, Boston, 23 September 2013.

Dale Miller is on the Advisory Board for LICS (for 2012 - 2015) and is a member of the Steering Committee of CPP since 2012.

Dale Miller gave invited departmental colloquia at the College of Engineering and Computer Science, Australian National University, 14 May and the Department of Mathematics and Computer Science, Freie Universität Berlin, 22 February.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: Stéphane Graham-Lengrand teaches 50 hours (eq. TD) in L3 at Ecole Polytechnique in the course "INF431: Algorithmique et programmation".

Master: Stéphane Graham-Lengrand teaches 36 hours (eq. TD) in M1 at Ecole Polytechnique in the course "INF551: Computer-aided reasoning", and 15 hours (eq. TD) in M2 at Master Parisien de Recherche en Informatique (MPRI) on "Curry-howard correspondence for classical logic".

Master: Dale Miller taught 12 hours at MPRI (Master Parisien de Recherche en Informatique) in the Course 2-1: Logique linéaire et paradigmes logiques du calcul.

Dale Miller was an invited lecturer at the CUSO Winter School in Mathematics and Computer Science "Proof and Computation", Les Diablerets, Switzerland, 27-31 January 2013.

8.2.2. Supervision

PhD: Nicolas Guenot, "Nested Deduction in Logical Foundations for Computation", Ecole Polytechnique, April 10 2013, supervisor Lutz Straßburger (thesis available at [12])

PhD: Ivan Gazeau, “Safe Programming in finite precision: Controlling the errors and information leaks”, Ecole Polytechnique, October 14 2013, supervisors: Dale Miller and Catuscia Palamidessi [11].

PhD: Mahfuza Farooque, “Automated reasoning techniques as proof search in sequent calculus”, Ecole Polytechnique, December 19 2013, supervisor: Stéphane Graham-Lengrand [29].

PhD in progress: Quentin Heath, since October 2013, supervisor: Dale Miller.

PhD in progress: Zakaria Chihani, since October 2012, supervisor: Dale Miller.

PhD in progress: Hernán Vanzetto, since October 2010, co-supervisors: Stefan Merz and Kaustuv Chaudhuri.

8.2.3. Juries

François Lamarche was member of the PhD jury of Pierre Rannou, Université Aix-Marseille, October 21 2013.

Dale Miller was a member of the PhD jury of the following three students during 2013: Mahfuza Farooque, Ecole Polytechnique 19 December 2013 (evaluator); Stéphane Zimmermann, University of Paris Diderot, 10 December 2013 (president); Matthias Puech, University of Bologna, 8 April 2013 (reporter).

Stéphane Graham-Lengrand was member of the PhD jury of Sophia Knight, École Polytechnique, September 20 2013.

PI.R2 Project-Team

7. Dissemination

7.1. Scientific Animation

7.1.1. Collective responsibilities

Pierre-Louis Curien is member of the Conseil Scientifique of the INSII (CNRS). He is also a member of the Conseil Scientifique of CIRM (since June 2013).

7.1.2. Editorial activities

Pierre-Louis Curien is co-editor in chief of Mathematical Structures in Computer Science, and is an editor of Higher-Order and Symbolic Computation.

7.1.3. Program committees and organising committees

Alexis Saurin has been co-chair of the program committee and editor of the proceedings of the workshop *Control Operators and their Semantics* (COS'13, organized at RDP 2013, http://cos2013.di.unito.it and http://rvg.web.cse.unsw.edu.au/eptcs/content.cgi?COS2013). The proceedings were published by EPTCS.

Alexis Saurin has been a member of the scientific committee of the Summer School *Linear Logic and Geometry of Interaction* (http://www.logoi.fr/events/school) which took place in Torino as a satellite event of CSL 2013.

Alexis Saurin is a PC member of GaLoP 2014 (International Workshop on Games and Logic for Programming) which will take place during ETAPS 2014 in Grenoble.

Hugo Herbelin, Pierre Letouzey and Matthieu Sozeau are co-organizing and co-chairing the TYPES'14 conference in Paris in May.

Matthieu Sozeau was in the PC of DTP'13, JFLA'13 and JFLA'14. He is in the newly formed steering committee of the DTP workshop https://www.pps.univ-paris-diderot.fr/dtp/.

Matthieu Sozeau co-organized a (private) meeting at POPL'14 in San Diego, there were 30 participants. He gave a talk on the upcoming 8.5 version of Coq and a tutorial.

Hugo Herbelin organized with Gyesik Lee a workshop on constructive reverse mathematics in Seoul, March 2013.

Yves Guiraud and Philippe Malbos are organisers of the 5-weeks programme Mathematical Structures of Computation, held in Lyon in January-February 2014, and supported by the Labex MILYON. They are also organisers of the second week, Algebra and Computation, while Pierre-Louis Curien and Hugo Herbelin organised the first week, Recent Trends in Type theory.

Pierre-Louis Curien, Hugo Herbelin and Paul-André Melliès are the organisers of the IHP trimester Semantics of proofs and certified mathematics, to be held next spring. They also organise a spring school at CIRM preceding the trimester.

Pierre-Louis Curien is member of the steering committee of the conferences Typed Lambda Calculi (TLCA) and Applications and of the international workshops Games for Logic and Programming Languages (GaLop).

7.1.4. Jury participation

Alexis Saurin was an examinor for the computer science oral at the entrance exam for Ecoles normales supérieures and a member of the jury for Ecole normale supérieure de la rue d'Ulm.

Alexis Saurin has been member of the Jury for LMFI Master.

7.1.5. Invited talks

Hugo Herbelin gave an invited talk on proving Gödel's completeness theorem with side-effects at the conference TLCA'13 in Eindhoven.

Philippe Malbos was invited speaker at the Sao Paulo - Lyon Algebra meeting, in October 2013.

Pierre-Louis Curien was an invited speaker at Glynn Winskel's anniversary workshop in Cambridge (where he presented his joint work with Garner and Hofmann on coherence issues in type theory), at the workshop Higher structures in China (Lanzhou, August), where he presented homotopical completions and reductions, at the International Symposium on Domain Theory, where he presented Thomas Ehrhard's result "Scott is the extensional collapse of Rel", and at the Loday's Mathematical Legacy conference in Strasbourg as well as at the Algebra and Computation workshop in Lyon where he presented his work on languages for operads and related structures.

7.1.6. Presentation of papers

Philippe Malbos has presented [16] at RTA 2013.

Lourdes González presented [14] at TYPES 2013.

Yann Régis-Gianas presented [14] at ITP 2013.

7.1.7. Other presentations

Yves Guiraud gave a talk on "Coherent presentations of Artin monoids" during the Journées PPS in September 2013.

Pierre Boutillier gave a talk on "An abstract machine to conceal strong reduction and fixpoints" during the journées PPS.

Yann Régis-Gianas presented the CerCo european project at two satellite workshops of HIPEAC (Berlin) in March 2013 and ETAPS (Roma) in April 2013.

Hugo Herbelin gave two lectures on reducibility candidates and their relation with completeness proofs to the Réalisabilité à Chambéry #6 workshop in June.

Hugo Herbelin gave a talk on the development of Coq at the Coq workshop '13 in Rennes.

Hugo Herbelin gave a talk at FOMCAF 2013 in Padova on the status of equality in type theory.

Hugo Herbelin gave a talk at TYPES 2013 in Toulouse on the status of equality in type theory.

Hugo Herbelin gave a talk at PCC 2013 in Toulouse on the Computational interpretation for the big five systems of reverse mathematics (joint work with Gyesik Lee and Keiko Nakata).

Matthieu Sozeau gave a talk at TYPES 2013 in Toulouse on universe polymorphism.

Matthieu Sozeau gave a talk at the TYPEX meeting in Paris on universe polymorphism.

Ludovic Patey gave a talk on Probabilistic Algorithms and Ramsey-Type Principles in Reverse Mathematics at the Workshop in Type Theory, in Séoul, on Rainbow Ramsey theorem for pairs at Computability in Europe, Milano, and on Classifying principles by the no randomized algorithm property at Logic Colloquium, Évora.

Jaime Gaspar gave a talk on Krivine's classical realisability and the unprovability of the axiom of choice and the continuum hypothesis at the 6th Young Set Theory Workshop 2013, Oropa, Italy. He gave a talk on "Refuting" Cantor at the Logic Colloquium 2013, Évora, Portugal.

7.1.8. Talks in seminars

Yves Guiraud gave three talks on "Coherent presentations of Artin monoids" at the Groupe de Travail Catégories supérieures, polygraphes et homotopie, PPS, Paris 7, in May-June 2013.

Matthieu Sozeau gave a talk on universe polymorphism at the Coq working group in Paris.

Alexis Saurin gave a talk at "Journées PPS" in september 2013 on linear head reduction and call-by-need, entitled "Éloge de la paresse".

Guillaume Claret gave a talk at Gallium on the Cybele plugin to do proofs by reflection in Coq using the extraction mechanism.

Guillaume Munch-Maccagnoni gave a talk on duploids at the PPS days in September 2013.

Zena Ariola presented a talk on Call-by-need: reduction, continuation passing style and abstract machines at Paris 7 University, 20 December 2012, and at Inria Saclay, 27 February 2013.

Jaime Gaspar gave a talk on Formalising ZF $\subseteq$ ZF$_\varepsilon$ in Paris, and at the Mathematical Logic Seminar, Lisbon. He gave a talk on Proof interpretations: what they are and what they are good for, at Junior Seminar, Rocquencourt, and at Parsifal team seminar, Palaiseau. He gave a talk on Krivine's classical realizability (see also above) at Technical University of Darmstadt, Darmstadt, and at University of Applied Sciences, Wiesbaden.

7.1.9. Attendance to conferences, workshops, schools,...

Yves Guiraud and Philippe Malbos attended RTA 2013, Eindhoven, in June.

Pierre Boutillier, Alexis Saurin and Pierre-Marie Pédrot attended the JFLA 2013 conference in Aussois.

Pierre Boutillier and Lourdes González attended the Coq workshop 2013 in Rennes.

Pierre Boutillier attended ICFP and DTP 2013 in Boston.

Lourdes González attended the Workshop on Formal Meta-Theory organized by the Parsifal team (Lix and Inria) the 5-6th March 2013.

Lourdes González, Guillaume Claret and Pierre-Marie Pédrot attended TYPES 2013 in Toulouse.

Yann Régis-Gianas, Guillaume Claret and Lourdes González attended ITP 2013 in Rennes.

Lourdes González and Pierre-Marie Pédrot attended the Summer School on Linear Logic and Geometry of Interaction in Turin.

Lourdes González attended CSL 2013 and its satellite events in Turin.

Pierre Letouzey attended the Coq workshop 2013 in Rennes.

Matthieu Sozeau attended the JFLA'13 in Aussois.

Matthieu Sozeau attended the Coq workshop 2013 and ITP 2013 in Rennes.

Matthieu Sozeau attended the TYPES 2013 conference in Toulouse.

Matthieu Sozeau attended the POPL'14 conference in San Diego.

Pierre Letouzey, Matthieu Sozeau, Lourdes González, Gullaume Munch and Pierre-Marie Pédrot attended Pierre-Louis Curien's 60th birthday meeting in Venice.

Matthieu Sozeau attended the Conference on Type Theory, Homotopy Theory and Univalent Foundations at the Centre de Recerca Matemàtica in Barcelona.

Guillaume Claret attended the EJCP 2013 school at Saint-Malo and Rennes.

Alexis Saurin attended BLL, a workshop on Bounded Linear Logic, in November 2013.

Zena Ariola attended POPL 2013, Rome.

Jaime Gaspar attended Proof Theory in Lisbon (a one-day workshop), and a workshop on Reverse Mathematics in Paris.

7.1.10. Groupe de travail Théorie des types et réalisabilité

Pierre-Marie Pédrot gave a talk on a classical realizability account of the Dialectica transformation, as well as a dependent version of it, in November.

Matthieu Sozeau gave a talk on a groupoid interpretation in March.

This year's other internal speakers were Hugo Herbelin, Philippe Malbos, and the external speakers were Maribel Fernández (King's College, London), Gregory Malecha (MIT), Marc Lasson (then postdoc at Cambridge Univ.), Keiko Nakata (Institute of Cybernetics, Tallinn), Cyril Cohen (Univ. of Göteborg), Eduardo Bonelli (Universidad Nacional de Quilmes), Barbara Petit (Sardes team, Inria Grenoble), Lionel Rieg (ENS Lyon), Fernando Ferreira (Univ. of Lisbonne), Chantal Keller (Univ. of Aarhus), Matthias Puech (Univ. of Aarhus), Dominic Hughes (Stanford University), Thomas Braibant (Gallium team), and Alexander Kreuzer (ENS Lyon).

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence: Pierre Boutillier has a temporary research and teaching position (A.T.E.R) at University Paris 7 for the academic year 2013–2014. He teaches this year Programmation fonctionnelle (L3) and Analyse lexicale et syntaxique (L3).

Master: Compilation, (Boutillier) 1/4, M1, Université Paris Diderot.

Master: Assistants de Preuve (Sozeau), 9, M2, Université Paris Diderot.

Master: Functional Programming and Type Systems (Regis-Gianas), 12, M2, Université Paris Diderot.

Master: Lambda-calculus (Saurin), 24H, M2 of Mathematics "Logique Mathématique et Fondements de l'Informatique", Université Paris Diderot.

Master Pierre-Louis Curien teaches in the course Models of programming languages: domains, categories, games of the MPRI (together with Thomas Ehrhard and Paul-André Melliès).

7.2.2. Supervision

Internship: Yves Guiraud has supervised the M2 internship of Maxime Lucas.

Internship: Alexis Saurin has supervised the internship of Fanny He.

Internship: Alexis Saurin has supervised (with Claudia Faggian) the M2 internship of Amina Doumane.

PhD in progress: Pierre Boutillier, Représentation des effets et inférence de type dans le cadre du développement d'un langage de programmation à types riches, September 2010, Hugo Herbelin.

PhD in progress: Lourdes del Carmen González Huesca, Un langage de tactiques typées pour Coq, December 2011, Hugo Herbelin and Yann Régis-Gianas.

PhD in progress: Guillaume Claret, Programmation avec effets en Coq, September 2012, Hugo Herbelin and Yann Régis-Gianas.

PhD in progress: Pierre-Marie Pédrot, Logique linéaire et types dépendants, september 2012, supervised by Alexis Saurin and Hugo Herbelin.

PhD in progress : Cyrille Chenavier, supervised by Yves Guiraud and Philippe Malbos.

PhD in progress : Maxime Lucas, supervised by Yves Guiraud and Pierre-Louis Curien.

PhD defended: Guillaume Munch-Maccagnoni, Syntaxe et modèles d'une composition non-associative des programmes et des preuves, Université Paris Diderot - Paris 7, December 10 2013, Pierre-Louis Curien and Thomas Ehrhard. [11]. Hugo Herbelin was a member of the jury.

7.2.3. Juries

Pierre-Louis Curien was referee and Yves Guiraud was jury member for the PhD defence of Pierre Rannou ("Réécriture de diagrammes et de Sigma-diagrammes", Univ. Aix-Marseille).

Pierre-Louis Curien was jury member of the thesis of Florian Hatat ("Jeux graphiques et théorie de la démonstration", Univ. Chambéry).

Pierre-Louis Curien was (as thesis director) in the jury of the theses of Stéphane Zimmermann (“Vers une ludique différentielle”, Univ. Paris Diderot) and of Alexis Goyet (“Le lambda lambda-bar calcul, un calcul dual pour les stratégies non contraintes”, Univ. Paris Diderot).

Pierre Letouzey was a referee for the PhD thesis of Pierre-Nicolas Tollitte in December 2013 (“Extraction de code fonctionnel certifié à partir de spécifications inductives”, CNAM), while Hugo Herbelin was a member of this PhD committee.

7.3. Popularization

Yann Régis-Gianas organised the "Fête de la Science" event for the computer science department of the University Paris 7.

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 gave several conferences about computer science in several primary schools of Paris.

SUMO Team

9. Dissemination

9.1. Scientific Animation

Éric Fabre was evaluator of the first round of the ANR call for projects, 2013. He is also a regular reviewer for the Ministry of Research and Innovation, through the Credit Impot Recherche program (support to industrial research through tax reductions).

Éric Badouel is Associate Editor of the ARIMA journal, member of the Board of SARIMA and of the Steering Committee of LIRIMA. He is the Secretary of the Permanent Committee of the CARI.

Nathalie Bertrand is elected member of the Steering Committee of QEST, international conference on Quantitative Evaluation of Systems. She is also on the Steering Committee of the international workshop QAPL. She has served this year on the Programme Committee of MSR'13, MFCS'13, QEST'13 and QAPL'13. She is member and scientific secretary of the Gilles Kahn PhD award committee.

Thierry Jéron was PC member of ACM SAC-SVT 2014, PECCS 2014, MAROC 2013, TAP 2013, RV 2013. He was co-chairman of a Dagstuhl seminar on Symbolic Methods in Testing (January 2013). He is member of the steering committee of Movep'2014 in Nantes (July 2014). He is member of the IFIP Working Group 10.2 on Embedded Systems. He gave an invited lecture on "Model-based conformance test generation for timed systems" at the workshop MAROC'2013.

Loïc Hélouët was co-organizer with Hervé Marchandof the MSR 2013 Conference. He is member of the program committee of the SDL conference. In 2013, he was also reviewer for the following conferences: SDL, TACAS, CONCUR, MOVEP, and journals : SOSYM, TCS. He is also scientific coordinator of the DISTOL associated team. He co-organizes (with N. Bertrand, F. Schwarzentruber, D. Cachera and J.-P. Talpin) the 68NQRT seminar at IRISA/Inria Rennes, a weekly event that proposes talks in the domain of theoretical computer science (around 40 talks each year from worldwide participants). He is *référent chercheur* for the Inria Rennes research center, helping researchers that face difficulties during their carreer. He was part of the committee for the selection of a *maître de conférences* position at ISTIC in May 2013.

Hervé Marchand member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. He is member of the steering committee of MSR (Modélisation de systèmes réactifs). He was co-organizer with Loïc Hélouëtof MSR 2013 in Rennes (13-15 November 2013). He was PC member of DCDS Conference and PC chair with Loïc Hélouëtof MSR 2013. He is PC member of the forthcoming WODES conference and IFAC World Congress in 2014. He was reviewer for Automatica, Transaction automatic and control, Discrete Event dynamical systems as well as CDC, ACC conference.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Éric Fabre

Master: ASR: introduction to distributed systems and algorithms, 12h, M2, Univ. Rennes 1, France.

Master: Information theory, 30h, M1, Ecole Normale Superieure de Rennes, France.

Nathalie Bertrand

Master: Advanced verification techniques, 15h (eq. TD), M2, ISTIC, Université de Rennes 1, France.

Agreg: Formal languages, 27h (eq. TD), M2, Ecole Normale Superieure de Rennes, France.

Loïc Hélouët

Licence: JAVA programming, 37h, INSA Rennes, France.

Agreg: Finite automata, and flow algorithms, 8h (eq. TD), M2, ENS Rennes, France.

9.2.2. Supervision

HdR: Loïc Hélouët, *Scenario Automata: theory and applications* , Rennes 1 University, 17th May 2013.

PhD: Carole Hounkonnou, *Auto-diagnostic actif dans les réseaux de télécommunications*, Rennes 1 University, 12th July 2013, supervised by Éric Fabre.

PhD: Rouwaida Abdallah, *Implémentabilité de systèmes distribués décrits à l'aide de scénarios*, ENS Cachan antenne de Bretagne, 16th July 2013, supervised by Loïc Hélouët and Claude Jard.

PhD: Amélie Stainer, *Contribution to the Verification of Timed Automata: Determinization, Quantitative Verification and Reachability in Networks of Automata*, Rennes 1 University, 25th November 2013, supervised by Thierry Jéron and Nathalie Bertrand.

PhD: Aurore Junier, *Performance and stability analysis in telecommunication networks*, Rennes 1 University, 16th December 2013, supervised by Anne Bouillard and Claude Jard.

PhD in progress (Defense on January 7th, 2014): Sébastien Chédor, *Diagnostic, opacité et test de conformité pour des systèmes récursifs.*, started in September 2009, supervised by Thierry Jéron and Christophe Morvan.

PhD in progress: Mohamadou Lamine Diouf, *Opacité des artefacts dans un système workflow*, started in spring 2011, supervised by Éric Badouel and colocated with Dakar Université Cheik Anta Diop (Senegal).

PhD in progress: Srinivas Pinisetty, *Runtime validation of critical control-command systems*, started in December 2011, supervised by Hervé Marchand and Thierry Jéron.

PhD in progress: Paulin Fournier, *Parameterized verification of networks of probabilistic processes*, started in September 2012, supervised by Thierry Jéron and Nathalie Bertrand.

PhD in progress: Bruno Karelovic, *Approximated analysis for checking Stochastic Models and Games*, started in November 2012, supervised by Blaise Genest and Wieslaw Zielonka.

9.2.3. Juries

Éric Fabre was reviewer of the PhD thesis of Fabien Kuntz, "Optimization of the monitoring of avionic systems through enhanced diagnosis performances," LABRI and University Bordeaux 1, July 2013. He also reviewed the PhD thesis of Leila Bennacer, "Contribution to self-diagnosis methods in large scale communication networks," University Paris-Est Creteil, Dec. 2013.

Thierry Jéron was member of the PhD defense jury of Aymeric Hervieu (Dec. 2013, Université Rennes 1).

Hervé Marchand was a member of the PhD defense juries of Mohammed Ali Kammoun (LAGIS, Metz) in July 2013 and of Xin An (Inria Rhones Alpes, Grenoble) in October 2013.

9.3. Popularization

Loïc Hélouët contributed to a vist of young pupils (3e) visiting IRISA to discover a research environment in February 2012. He did a short interactive presentation (1 hour) of his research theme, and of the duties of a researcher.

Éric Fabre gave a survey presentation about failure diagnosis in telecommunication networks to the 2nd year students of ENST Bretagne (Brest) engaged in a research training track. This was followed by informal discussions about the every day life of a researcher.

TOCCATA Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Event Organization

- C. Marché organizer of the first DigiCosme Spring School (http://labex-digicosme.fr/Spring+School+2013 whose theme is *Program Analysis and Verification* in April 2013.
- C. Paulin, organizer with D. Pichardie and S. Blazy of the 4th Conference on Interactive Theorem Proving (http://itp2013.inria.fr/) in July 2013.
- C. Paulin, organizer with Zhong Shao (Yale Univ.) of the workshop "Certification of high-level and low-level programs" July 7-11, 2014, as part of the Institut Henri Poincaré thematic trimester on Semantics of proofs and certified mathematics https://ihp2014.pps.univ-paris-diderot.fr.

9.1.2. Editorial boards

- S. Boldo, member of the editorial committee of the popular science web site *interstices*, http://interstices.info/.
- J.-C. Filliâtre is member of the editorial board of the *Journal of Functional Programming*.
- C. Paulin, member of the editorial board of the *Journal of Formalized Reasoning*.

9.1.3. Learned societies

- J.-C. Filliâtre is a member of IFIP Working Group 1.9/2.15 (Verified Software)

9.1.4. Program committees

- É. Contejean, member of the program committee of the 24th International Conference on Automated Deduction (CADE 24, http://www.cade-24.info/),member of the program committee of the ACM SIGPLAN 2014 Workshop on Partial Evaluation and Program Manipulation (PEPM 2014, http://www.program-transformation.org/PEPM14), and member of the program committee of the 13th International Workshop on Termination (WST 2013, http://www.imn.htwk-leipzig.de/WST2013/).
- C. Marché, *Tool Chair* of the program committee of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013, Rome, Italy, http://www.etaps.org/index.php/2013/tacas), part of the ETAPS joint Conference. The tool chair is responsible for the evaluation and selection of tool papers and tool demonstrations, following precise guidelines given in the call for papers. This initiative of TACAS aims at making the selection of such submissions more accurate (http://www.etaps.org/index.php/2013/tacas/tacas13-tool-papers-menu).
- C. Paulin, member of the program committees of the fourth and fifth conferences on Interactive Theorem Proving (ITP 2013, http://itp2013.inria.fr/ and ITP 2014 http://www.cs.uwyo.edu/~ruben/itp-2014/).
- J.-C. Filliâtre is a member of the program committees of the 5th NASA Formal Methods Symposium (NFM 2013), Certified Programs and Proofs (CPP 2013), Symposium on Languages, Applications and Technologies (SLATE 2013), VeriSure: Verification and Assurance (2013), and the 5th Working Conference on Verified Software: Theories, Tools and Experiments (VSTTE 2013).
- A. Paskevich is a member of the program committee of the 3rd International Workshop on Proof Exchange for Theorem Proving (PxTP 2013) affiliated with the CADE-24 conference.

9.1.5. Invited Presentations

- J.-C. Filliâtre, "One logic to use them all", CADE-24, Lake Placid, USA, June 2013 [19].

- J.-C. Filliâtre, “Deductive Program Verification”, PLMW 2013, Rome, Italy, January 2013 [18].
- S. Boldo, “Formal proofs and the 1D wave equation”, MOISE seminar, Grenoble, January 10th.
- S. Boldo, “Formal verification of numerical programs”, long talk at the Journées du GDR IM, Lyon, January 21st.
- É. Contejean, “A first Coq mechanized course in relational databases”, ANR Typex, Paris, December 17th.
- C. Lelay, “Real Analysis in Coq”, LIX PhD seminar, Palaiseau, September 27th.
- G. Melquiond, “Formal Proof of Numerical Properties and Automation”, CEA LSL seminar, Gif-sur-Yvette, February 26th.
- G. Melquiond, “Formal Proof and Interval Arithmetic, a Virtuous Circle”, College of Engineering, University of Texas, El Paso, USA, April 12th.
- G. Melquiond, “What is in Store for Coq.Interval”, ANR Tamadi, Lyon, July 16th.
- G. Melquiond, “Automations for Verifying Floating-point Algorithms in Coq”, the 5th Coq Workshop, Rennes, July 22th.
- S. Conchon, “Cubicle: Design and Implementation of an SMT based Model Checker for Parameterized Systems”, SMT Workshop 2013, Helsinki, Finland, July 9th.
- A. Paskevich, “Deductive Program Verification with Why3”, IRISA seminar, Rennes, October 10th.
- S. Conchon and A. Paskevich, “Savoir-faire et logiciels open source — Toccata”, Open World Forum, “Rencontre Inria-Industrie sur la qualité logicielle”, Montrouge, October 4th.
- C. Dross, “Defining new theories in SMT solvers using fisrt-order axioms with triggers”, CEA LSL seminar, Gif-sur-Yvette, November 12th.

9.2. Interaction with the scientific community

9.2.1. Collective Responsibilities within Inria

- S. Boldo, elected member of the Inria Evaluation Committee. She was in the committee in charge of selecting the Inria permanent researchers (CR2) in Sophia and Saclay.
- S. Boldo was in the committee in charge of upgrading an Inria support staff at the IR level (*ingénieur de recherche*), which is the highest level for support staff.
- S. Boldo, member of the CLFP, *comité local de formation permanente*.
- S. Boldo and A. Charguéraud, members of the committee for the monitoring of PhD students (*commission de suivi des doctorants*).
- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- S. Boldo, member of the popularization committee, *comité de médiation scientifique*, of Inria.

9.2.2. Collective Responsibilities outside Inria

- A. Charguéraud is vice-president of *France-IOI*, a non-profit organization in charge of the selection and the training of the French team to the International Olympiads in Informatics. France-IOI also provides online exercises in programming and algorithmics — in average, more than 70,000 such exercises are solved every month on the website.
- A. Charguéraud is a board member of the non-profit organization *Animath*, which aims at developing interest in mathematics among young students.
- É. Contejean and C. Marché, nominated members of the *“conseil du laboratoire”* of LRI since April 2010.
- É. Contejean, elected member of the *“section 6 du Comité National de la Recherche Scientifique”* since September 2012.

- C. Lelay, elected member of the *"conseil du laboratoire"* of LRI since November 2011.
- C. Lelay, elected representative of the students at the Doctoral School in Computer Science at University Paris-Sud from November 2011 to November 2013.
- C. Marché (since April 2007) and C. Paulin (since September 2010), members of the program committee of Digiteo Labs, the world-class research park in *Île-de-France* region dedicated to information and communication science and technology, http://www.digiteo.fr/. C. Marché, president of this committee since July 2013.
- C. Marché and S. Boldo, members of the *"jury de l'agrégation externe de mathématiques"* as experts in computer science, since 2012.
- G. Melquiond and C. Paulin, members of the *"commission consultative de spécialistes de l'université"*, Section 27, University Paris-Sud since April 2010.
- G. Melquiond, elected officer of the IEEE-1788 standardization committee on interval arithmetic since 2008.
- C. Paulin, scientific leader of Labex DigiCosme http://labex-digicosme.fr (Digital Worlds Distributed data, programs and architectures), a project launched by the French Ministry of research and higher education as part of the program "Investissements d'avenir", it involves the 14 research units in computer science and communications from the "Paris-Saclay" cluster.
- C. Paulin, president of the Computer Science Department of the University Paris-Sud https://www.dep-informatique.u-psud.fr/, since February 2012.
- C. Paulin, president of the assembly of directors of graduate schools at the Université Paris-Sud since September 2012.
- J.-C. Filliâtre is *correcteur au concours d'entrée à l'École Polytechnique* (computer science examiner for the entrance exam at École Polytechnique) since 2008.
- A. Paskevich is in charge (together with C. Bastoul in 2012–2013 and B. Cautis in 2013–2014) of Licence professionnelle PER (L3) at IUT d'Orsay, Paris-Sud University since September 2012.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Licence (L2): "Principes d'interprétation des langages", C. Dross (30h), Université Paris-Sud, France

Licence (L2): "Mathématiques pour l'Informatique" , C. Paulin (64h), M. Iguernelala (10h), A. Tafat (10h), Université Paris-Sud, France

Licence (L3): "Eléments de logique pour l'informatique", C. Paulin (32h), Université Paris-Sud, France

Licence (L3): "Programmation fonctionnelle", C. Dross (4h), Université Paris-Sud, France

Licence Professionnelle «Programmation en environnements répartis» (LP PER): "Programmation concurrente" (L3Pro), A. Paskevich (36h), IUT d'Orsay, Université Paris-Sud, France

Licence (L3): "Programmation fonctionnelle", M. Clochard (15h), ENSIIE, France

Master (M1): "Projet de Programmation", A. Tafat (42h), Université Paris-Sud, France

Master (M1): "Compilation", A. Tafat (28h), Université Paris-Sud, France

Master (M1): "Complément objet", A. Tafat (12h), Polytech, Université Paris-Sud, France

Master (M1): "Compilation", A. Tafat (12h), Polytech, Université Paris-Sud, France

Master (M1): "Projet de Compilation", A. Tafat (12h), Polytech, Université Paris-Sud, France

Master (M2Pro): "XML et Programmation Internet", A. Tafat (13h), Université Paris-Sud, France

Master (M2-agrégation): "Logique", C. Paulin (21h), Université Paris-Sud and ENS Cachan, France

Master Parisien de Recherche en Informatique (MPRI) https://wikimpri.dptinfo.ens-cachan.fr/doku.php: "Automated Deduction" (M2-5), S. Conchon (9h), É. Contejean (3h), Université Paris 7, France.

Master Parisien de Recherche en Informatique (MPRI) https://wikimpri.dptinfo.ens-cachan.fr/doku.php: "Proofs of Programs" http://www.lri.fr/~marche/MPRI-2-36-1/ (M2), C. Marché (12h), G. Melquiond (12h), Université Paris 7, France.

DUT (Diplôme Universitaire de Technologie): "Structures de données et algorithmique fondamentale" (S1), C. Lelay (38h, "moniteur" position), IUT d'Orsay, Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): "Introduction aux systèmes informatiques" (S1), A. Paskevich (97h), C. Lelay (30h), IUT d'Orsay, Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): "Programmation système" (S4), A. Paskevich (48h), IUT d'Orsay, Université Paris-Sud, France.

Teaching teachers ("Formation de formateurs") S. Boldo (3h) January 17th

École Jeunes Chercheurs en Programmation (EJCP 2013): J.-C. Filliâtre ,"Deductive Program Verification with Why3" (4h) http://why3.lri.fr/ejcp-2013/.

Licence: "Langages de programmation et compilation" (L3), J.-C. Filliâtre (36h), École Normale Supérieure, France

Licence: "INF421: Les bases de l'algorithmique et de la programmation" (L3) et "INF431" (L3), J.-C. Filliâtre (70h), École Polytechnique, France

9.3.2. Supervision

PhD: P. Herms, "Certification of a Tool Chain for Verification of C programs" [12], Univ. Paris-Sud Jan. 14, 2013, C. Marché, B. Monate (CEA-LIST)

PhD: M. Iguernelala, "Strengthening the heart of an SMT-solver: Design and implementation of efficient decision procedures" [13], Univ. Paris-Sud, June 10, 2013, S. Conchon, É. Contejean

PhD: A. Tafat, "Preuve par raffinement de programmes avec pointeurs" [14], Univ. Paris-Sud, Sep. 6, 2013, C. Marché

PhD in progress: C. Dross, "Theories and Techniques for Automated Proof of programs", since Jan. 2011, C. Marché, A. Paskevich, and industrial supervisors Y. Moy and J. Kanig (AdaCore company)

PhD in progress: A. Mebsout, "SMT-based Model-Checking", since Sep. 2011, F. Zaidi, S. Conchon

PhD in progress: C. Lelay, "Real numbers for the Coq proof assistant", since Oct. 2011, S. Boldo, G. Melquiond

PhD in progress: S. Dumbrava, "Towards data certification", since Oct. 2012, V. Benzaken (LRI), É. Contejean

PhD in progress: L. Gondelmans, "Obtention de programmes corrects par raffinement dans un langage de haut niveau", since Oct. 2013, J.-C. Filliâtre, A. Paskevich

PhD in progress: M. Clochard, "A unique language for developing programs and prove them at the same time", since Oct. 2013, C. Marché, A. Paskevich

9.3.3. Juries

C. Marché: president of the PhD committee of C. Keller, "A Matter of Trust: Skeptical Communication Between Coq and External Provers", (École Polytechnique, LIX laboratory, June 19, 2013)

C. Marché: reviewer, PhD committee of X. Shi "Certification of an Instruction Set Simulator" (University Grenoble, Verimag laboratory, July 10th, 2013)

C. Marché: president of the PhD committee of E. Tushkanova "Schematic calculi for the analysis of decision procedures" (University Besançon, FEMTO-ST laboratory, July 19th, 2013)

C. Marché: reviewer, PhD committee of H. Debrat "Certification formelle de la correction d'algorithmes de Consensus" (University Nancy, LORIA laboratory, Dec 6th, 2013)

C. Marché: president of HDR committee of S. Gérard "Ingénierie dirigée par les modèles" (University Paris-Sud, LISE laboratory of CEA-LIST, Dec 17th, 2013)

S. Conchon: president of the PhD committee of L. Gerard "Programmer le parallélisme avec des futures en Heptagon un langage synchrone flot de données et étude des réseaux de Kahn en vue d'une compilation synchrone" (University Paris-Sud, ENS, Sept. 25th, 2013)

S. Conchon: president of the PhD committee of J. Cheng "Stochastic Combinatorial Optimization" (University Paris-Sud, Nov. 8th, 2013)

S. Conchon: reviewer, PhD committee of M. Farooque "Automated reasoning techniques as proof-search in sequent calculus" (École Polytechnique, Dec. 19th, 2013)

J.-C. Filliâtre: reviewer, PhD committee of David Miguel Ramalho Pereira "Towards certified program logics for the verification of imperative programs" (Universidade do Porto, April 18, 2013)

J.-C. Filliâtre: reviewer, PhD committee of Jean Fortin "BSP-Why: a Tool for Deductive Verification of BSP Programs" (Université Paris Est, October 14, 2013)

J.-C. Filliâtre: reviewer, PhD committee of Maxime Denès "Formal study of efficient algorithms in linear algebra" (Université de Nice - Sophia Antipolis, November 20, 2013)

9.4. Industrial Dissemination

- As a final result of the Hi-Lite project, the Adacore company (Paris) implemented the new environment Spark2014 for the development of critical Ada software (http://www.spark-2014.org/), the successor of Spark, to be released in 2014. Part of this environment is the tool GnatProve which aims at formal verification. It translates annotated Ada code into the *Why3* intermediate language and then use the *Why3* system to generate proof obligations and discharge them with Alt-Ergo, or other available back-end provers.

9.5. Education, Popularization

- S. Conchon and J.-C. Filliâtre were involved in the writing of a new book supporting the new teaching program for the *"Classes préparatoires aux grandes écoles"* [39].
- S. Boldo and A. Charguéraud belong to the organization committee of the *Castor informatique*http://castor-informatique.fr/, an international competition to present computer science to pupils (from *6ème* to *terminale*). More than 170,000 teenagers played on the more than 30 proposed exercises in November 2013.
- Since April 2008, S. Boldo is member of the editorial committee of the popular science web site)i(: http://interstices.info/.
- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- S. Boldo, member of the popularization committee, *comité de médiation scientifique*, of Inria.
- S. Boldo was among the authors of a document [41] that describes the present and future of popularization at Inria.
- S. Boldo is responsible for a *mission doctorale* for popularization. She is in charge of Li Gong of the LIMSI laboratory: he wrote an Interstices article: http://interstices.info/traduction-automatique-statistique.
- S. Boldo, talk at the *Fête de la science* 2013 for the laboratory, October 11th.
- S. Boldo, talk for a general audience at the Courbevoie library, February 9th
- S. Boldo, talk for teenagers at the lycée Talma de Brunoy, April 23th

- S. Boldo, talk for mathematics teachers at Rocquencourt, June 5th
- S. Boldo, "speed-dating" with teenagers at the Halle Forum, October 18th, in an event called "Science au carré(e)".
- S. Boldo, article for the French blog celebrating 2013 as the "Mathematics of Planet Earth" year: http://mpt2013.fr/meme-les-ordinateurs-font-des-erreurs/.
- C. Lelay tried the 2013 mathematics test of the scientific Baccalaureate in Coq. After the test, a meeting was organized with some teachers and the produced proofs and results were presented.
- C. Paulin organised at the *Fête de la science* 2013 an action of Labex DigiCosme to promote the new course "Informatique and Sciences du Numériques" in high-school, a few selected projects developed by students as part of their curriculum were exhibited.

VERIDIS Project-Team

9. Dissemination

9.1. Scientific Animation

- Pascal Fontaine co-chaired the International Conference on Frontiers of Combining Systems (FroCoS 2013). He served on the program committee of the workshops PxTP 2013, SMT 2013, and the International Conference on Computer Aided Deduction (CADE 2013). He is an elected member of the SMT Steering Committee, and one of three SMT-LIB managers.
- Dominique Méry is
  - a member of the IFIP Working Group 1.3 on *Foundations of System Specification*,
  - head of the Doctoral School IAEM Lorraine for the University of Lorraine,
  - head of the Formal Methods department of the LORIA laboratory,
  - an expert for the French Ministry of Education (DS9),
  - an expert for the French Agence Nationale de la Recherche (ANR) and AERES.
  - He served on the program committees of FHIES, FM, ICECCS, ICFEM, iFM, and FACS.
- The academic duties of Stephan Merz in 2013 included:
  - member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*,
  - Inria representative in the Scientific Directorate of the International Computer Science Meeting Center in Dagstuhl,
  - delegate for the organization of conferences at Inria Nancy Grand-Est,
  - co-head of the PhD committee for computer science in Lorraine,
  - member of the program committees of iFM, Memocode, SAC, SBMF, and SEFM conferences, AFADL, AVoCS, Refinement, and SCSS workshops, member of the steering committee of AVoCS,
  - co-organizer of the VTSA summer school between Nancy, Saarbrücken, Luxembourg, and Liège,
  - president of the hiring committee for a professorship at Télécom Nancy and member of the hiring committee for professors at Université de l'Artois in Lens,
  - expert for the French Agence Nationale de la Recherche (ANR), German DFG, and Canadian NSERC.
- Thomas Sturm is a member of the Selection Committees for MSc and PhD students of the International Max-Planck Research School for Computer Science.
- Christoph Weidenbach is:
  - editor of JAR,
  - trustee of CADE Inc (elected 2009, reelected 2012),
  - member of the Appointment Decision Panel of FBK, Trento,
  - member of the Selection Committee of the Saarbruecken Graduate School in Computer Science,
  - member of Steering Committee *Bundeswettbewerb Informatik*,
  - co-organizer of the VTSA summer school between Nancy, Saarbrücken, Luxembourg, and Liège.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

The university employees of VeriDis have significant teaching obligations. We indicate the graduate courses they have been teaching this year.

- Dominique Méry gave courses in the Master program in Nancy on: formal system engineering, modeling and verification of systems, theoretical computer science, development of software systems, distributed algorithms.
- Marie Duflot-Kremer and Stephan Merz taught a course on algorithmic verification in the Master program in Nancy.
- Uwe Waldmann taught a course on Automated Reasoning at Saarland University.
- Christoph Weidenbach gave a course on Automated Reasoning II and lectured within the series "Perspektiven der Informatik" at Saarland University.

9.2.2. Supervision

- PhD: Henri Debrat, Certification formelle de la correction d'algorithmes de Consensus, Université de Lorraine. Supervised by Bernadette Charron-Bost and Stephan Merz, defended on December 6, 2013.
- PhD: Tianxiang Lu, Formal Verification of the Pastry Protocol, Université de Lorraine and Universität des Saarlandes. Supervised by Stephan Merz and Christoph Weidenbach, defended on November 27, 2013.
- PhD in progress: Manamiary Andriamiarina, Refinement Techniques for Distributed Algorithms, Université de Lorraine. Supervised by Dominique Méry, since 10/2010.
- PhD in progress: Noran Azmy, On the Automation of Proofs in TLAPS, Saarland University. Supervised by Christoph Weidenbach, since 11/2012.
- PhD in progress: Haniel Barbosa, Refutational Completeness in Satisfiability Modulo Theories, Université de Lorraine. Supervised by Pascal Fontaine and Stephan Merz, since 12/2013.
- PhD in progress: Marek Košta, Computational Logic, Universität des Saarlandes. Supervised by Thomas Sturm, since 11/2011.
- PhD in progress: Hernán Vanzetto, SMT Techniques for TLA$^+$ Proof Obligations, Université de Lorraine. Supervised by Kaustuv Chaudhuri and Stephan Merz, since 10/2010.

9.2.3. Juries

Stephan Merz wrote reports on the following PhD theses:

- Pierre-Emmanuel Cornilleau: *Certification of Static Analysis in Many-Sorted First-Order Logic*, ENS Cachan-Bretagne;
- Mélanie Jacquel: *Automatisation des preuves pour la vérification des règles de l'Atelier B*, CNAM Paris;
- Chantal Keller: *A Matter of Trust: Skeptical Communication Between Coq and External Provers*, Ecole Polytechnique;
- Yan Zhang: *Semi-Automatic Controller Design in a Java-like Language*, Université Paris 6.

He also was a member of the PhD committees of Dorin Maxim and Faqing Yang in Nancy.

Thomas Sturm was a member of the PhD committee of Evgeny Kruglov in Saarbrücken.

9.3. Popularization

Marie Duflot-Kremer, Pascal Fontaine, and Stephan Merz presented some of the subjects and techniques that underly formal verification of protocols and algorithms at events like "Fête de la Science". Using wooden puzzles, Sudoku sheets or boxes with locks, they explained how real-life problems can be represented in logical form and then solved using automated tools based on formal logic.

Marie Duflot-Kremer presented exercise sessions for high school students on “conducting a police investigation using databases” and “discovering Turing machines with Lego bricks”. She is also a member of the steering committee preparing an itinerant exposition intended for explaining computer science to high-school students.

Thomas Sturm, Uwe Waldmann, and Christoph Weidenbach are involved in the “Computer Science Research Days” which take place every year. Gifted students from all over Germany can actively participate in current research themes within the Max Planck Institute for Informatics, the Computer Science Department of Saarland University and the German Research Center for Artificial Intelligence. The goal is to fill young people with enthusiasm for the subject of computer science as well as to discover and support the development of new talent.

CARTE Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Conference organization and program committee

Mathieu Hoyrup was in the Program Committee of Computability, Complexity and Randomness (CCA) 2013. He is guest editor for the post-proceedings of CCA 2013, special issue of Logical Methods in Computer Science. He has been invited to organize the special session Algorithmic Randomness of the conference Computability in Europe (CiE) 2013.

Simon Perdrix is a member of the Program Committee of the first Workshop on Parallel Quantum Computing (ParQ).

Guillaume Bonfante was in the Program Committee of Malware 2013 and Symposium on Foundations & Practice of Security (FPS) 2013.

The Carte Team has organized a few conferences and workshops in Nancy this year:

- Journées Calculabilités 2013, April
- Analysis, Randomness and Applications (ARA) 2013, June.
- Computability and Complexity in Analysis (CCA) 2013, July.
- Journées Informatique Quantique, October.

9.1.2. Talks

Emmanuel Jeandel gave an invited Talk at the conference (Computability, Complexity and Randomness (CCR) 2013) on entropy of Turing machines. He also presented his work on multidimensional symbolic dynamics in the PIMS Workshop on Automata Theory and Symbolic Dynamics.

Guillaume Bonfante was invited to present his work to workshop “Proof Theory and Rewriting” (Kanazawa, february) and “Journées Francophones d’Investigation Numérique” (Neuchâtel, october).

Guillaume Bonfante, Hugo Férée and Jean-Yves Marion were invited to workshop “Advances in implicit computational complexity” in Shonan Village in november.

Mathieu Hoyrup, Emmanuel Hainry, Emmanuel Jeandel, were invited to present their work to (workshop DySyCo) in Lyon, december 2013.

Emmanuel Hainry presented *Complexité d’ordre supérieur, de l’Analyse Récursive aux Basic Feasible Functionals* at the Séminaire d’algorithmique et de complexité du plateau de Saclay (http://www.lix.polytechnique.fr/~bodirsky/seminaire/) in LIX, Palaiseau in June 2013.

9.1.3. Referees

Emmanuel Hainry reviewed articles for the journal *Computability*, for *SIAM Journal on Computing*, and for the *STACS 2014* conference.

Emmanuel Jeandel reviewed articles for the *LICS 2013* and the *STACS 2014* conference.

Romain Péchoux reviewed articles for the *WORDS 2013* conference

Mathieu Hoyrup reviewed articles for the CiE 2013, STACS 2014, STOC 2014 conferences and the journals Logical Methods in Computer Science and Theory of Computing Systems.

9.1.4. Others

Isabelle Gnaedig is member of the scientific mediation committee of Inria Nancy Grand-Est and researcher social referee at Inria Nancy-Grand Est.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Unless specified otherwise, all teaching is done at Université de Lorraine, France.

Licence :

- Guillaume Bonfante
  - Java, L3, Mines Nancy
- Emmanuel Hainry
  - Operating Systems, 60 hours, L1, IUT Nancy Brabois
  - Algorithms and Programs, 60 hours, L1, IUT Nancy Brabois
  - Object Oriented Programming, 24 hours, L1, IUT Nancy Brabois
  - Databases, 24 hours, L2, IUT Nancy Brabois
  - Complexity, 28 hours, L1, IUT Nancy Brabois
  - Algorithmics, 12 hours, DU PFST (eq. L1), IUT Nancy Brabois
- Emmanuel Jeandel
  - Statistics for Computer Science, 46 hours, L3 Informatique
  - Linear Programming, 46 hours, L3 Informatique
  - Algorithmics and Programming 1, 60 hours, L1 Maths-Info
  - Algorithmics and Programming 4, 30 hours, L3 Informatique
  - Networking, 20 hours, L2 and L3 Informatique
- Romain Péchoux
  - Introduction to OO programming, 55 hours, L3 MIASHS parcours MIAGE.
  - Databases, 42 hours, L3 SG, ISAM-IAE
  - Propositional logic, 35 hours, L1 MIASHS
  - Algorithmic complexity, 30 hours, L3 MIASHS parcours MIAGE, IGA Casablanca, Marocco.

Master

- Guillaume Bonfante
  - Modelling and UML, M1, Mines Nancy
  - Video Games, M1, Mines Nancy
  - Semantics, M1, Mines Nancy
  - Safety of Software, M2, Mines Nancy
- Isabelle Gnaedig
  - Design of Safe Software, Coordination of the module, M2, Telecom-Nancy
  - Rule-based Programming, 20 hours, M2, Telecom-Nancy
- Emmanuel Jeandel
  - Algorithmics and Complexity, M1 Informatique and M1 ENSEM, 60 hours
  - Combinatorial Optimization, M1 Informatique, 30 hours.
- Romain Péchoux
  - Mathematics for computer science, 20 hours, M1 SC
  - Advanced Java, 52 hours, M1 MIAGE
- Simon Perdrix
  - Pépites Algorithmiques — Informatique Quantique, 14 hours, M1/M2, Ecole des Mines de Nancy.

9.2.2. Supervision

PhD : Joan Calvet, Analyse Dynamique de Logiciels Malveillants, Université de Lorraine and Ecole Polytechnique de Montreal, defended August 23rd, supervised by Jean-Yves Marion and José M. Fernandez.

PhD in progress: David Cattanéo, Combinatorial Modelization in Quantum Computation and Generalized Cover Problems, started sept. 2012, Pablo Arrighi (director), Simon Perdrix (co-advisor)

PhD in progress: Hugo Férée, Computational Complexity in Analysis, defense planned in December 2014, Jean-Yves Marion (director) and Mathieu Hoyrup (co-advisor).

PhD in progress: Hubert Godfroy, Semantics of Self-modifying Programs, Jean-Yves Marion

PhD in progress: Jérôme Javelle , Quantum Cryptography: Protocols and Graphs, started Jan. 2011, Pablo Arrighi (director), Mehdi Mhalla (co-advisor), Simon Perdrix (co-advisor)

PhD in progress: Thanh Dinh Ta, Malware Algebraic Modeling and Detection, started Sept. 2010, Jean-Yves Marion (director) and Guillaume Bonfante (co-advisor)

PhD in progress: Aurélien Thierry, Morphological Analysis of Malware, started Oct. 2011 supervised by Jean-Yves Marion.

9.2.3. Juries

Isabelle Gnaedig:

- participation to the Telecom-Nancy admission committee.

Emmanuel Jeandel

- Selection committee for a research assistant position in Nice (MCF 1114).
- Jury of Razvan Barbulescu's PhD Defense on "Algorithmes de logarithmes discrets dans les corps finis", defended in Université de Lorraine, December 5th.

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.

This year, in particular, the center participated to organization of mathematics competitions and projects for high school students, to conferences for computer science high school teachers, to the "Fête de la Science", to the "Moments d'invention" exhibition of the "Nancy Renaissance" event, and received several high school classes in various research teams of Inria Nancy Grand-Est. Details can be found at https://iww.inria.fr/NanSciNum/#.UsGBEWTuKY8.

CASSIS Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorial board

- Information & Computation (Véronique Cortier)
- Journal of Computer Security (Véronique Cortier)

9.1.2. Conferences

- FroCoS 2013, 9th Symposium on Frontiers of Combining Systems, 18–20 September 2013, Nancy, France, (Christophe Ringeissen, conference chair)

9.1.3. Program committees

- Fabrice Bouquet: ICST 2013 (Publicity Chair), MoDeVVA 2013
- Véronique Cortier: CSF 2013 (PC Chair), CCS 2013, LICS 2013, POST 2013
- Frédéric Dadeau : CSTVA'2013 (PC Chair), QSIC'2013.
- Abdessamad Imine: AICCSA 2013 (co-chair), CIIA 2013, DEXA 2013, DEXA 2014
- Steve Kremer: ACNS 2014, POST 2014 (PC Chair), Security Track of ACM SAC 2014 (PC Chair), ESORICS 2013, ICICS 2013, ISPEC 2013, POST 2013, RV 2013
- Christophe Ringeissen: CADE-24, FroCoS 2013, UNIF 2013, UNIF 2014 (co-chair)
- Michael Rusinowitch: LATA 2013, CRISIS 2013, ESSOS DS 2013, GRSRD 2013.
- Laurent Vigneron: UNIF 2013.

9.1.4. Steering committees

- Véronique Cortier: FCS (Chair), CSF
- Steve Kremer: CSF, ETAPS, POST

9.1.5. Spring school

- Spring School on Trusted and Secure Composite Services, 27–31 May 2013, Malaga, Spain, (Abdessamad Imine, Lecturer)
- JDEV'2013 National Day for Software development, 4–6 September 2013, Ecole polytechnique (Palaiseau), France (Bouquet F., Gauthier J.-M. and Enderlin I., 5 tutorials and 1 Lecturer) - 500 participants.
- School of INRA on the Testing for Software Development, in PEPI IDL 2013 (*"Partage d'Expérience et de Pratiques en Informatique" visant l'"Ingénierie Développement Logiciel"*), 9–12 December 2013, Ecully (69) France (Bouquet F., Gauthier J.-M. and Enderlin I., 3 days of tutorials) - 30 participants.
- 13th International School on Foundations of Security Analysis and Design, 2–7 September 2013, Bertinoro, Italy (Mathieu Turuani, Tutorial).
- AFADL'2013 (*"Approches Formelles dans l'Assistance au Développement de Logiciels"*), during the GDR - GPL - CIEL - AFADL Days, 2–5 april 2013, Nancy, France (Mathieu Turuani, Tutorial) - 135 participants.

9.1.6. Working groups

- GT-Verif, Verification, GDR IM Working Group (Véronique Cortier, chair)

- IFIP WG-1.7 Foundations of Security Analysis (Véronique Cortier, vice-Chair)
- IFIP WG-1.6 - Term Rewriting (Michael Rusinowitch, Laurent Vigneron)
- MTV2, Testing Methods for Verification and Validation, GDR GPL Working Group (Frédéric Dadeau, co-chair)
- FORWAL, Formalisms and Tools for Verification and Validation, GDR GPL Working Group (Pierre-Cyrille Héam, co-chair)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence :
  - Frédéric Dadeau, Programming, 37 hours (ETD), L1, Université de Franche-Comté
  - Frédéric Dadeau, Databases, 39 hours (ETD), L1, Université de Franche-Comté
  - Frédéric Dadeau, Web Languages, 24 hours (ETD), L2, Université de Franche-Comté
  - Frédéric Dadeau, Object-Oriented Modelling and Design, 44 hours (ETD), L3, Université de Franche-Comté
  - Alain Giorgetti, Logics and Deduction, 52 hours (ETD), L2, Université de Franche-Comté, France.
  - Alain Giorgetti, Formal Methods, 81 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Formal Languages, 65 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3, Université de Franche-Comté, France
  - Olga Kouchnarenko, Parsing Algorithms and XML, 30 hours (ETD), L3, Université de Franche-Comté, France
- Master :
  - Fabrice Bouquet, Artificial Intelligence (also in e-learning), 53 hours (ETD), M2, Université de Franche-Comté
  - Fabrice Bouquet, Compilation, 54 hours (ETD), M2, Université de Franche-Comté
  - Fabrice Bouquet, Testing (also in e-learning), 71 hours (ETD), M2, Université de Franche-Comté
  - Frédéric Dadeau, Testing, 13 hours (ETD), M2, Université de Franche-Comté
  - Alain Giorgetti, Program Proofs, 58 hours (ETD), M1, Université de Franche-Comté, France.
  - Alain Giorgetti, Decision Procedures, 13 hours (ETD), M2, Université de Franche-Comté, France.
  - Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.
  - Christophe Ringeissen, Decision Procedures for Software Verification, 24 hours (ETD), M2 Computer science, Lorraine University, France.
  - Laurent Vigneron, Security of information systems, 15 hours (ETD), M2 Computer science, Lorraine University, France.
  - Laurent Vigneron, Formal methods, 24 hours (ETD), M2 MIAGE, Lorraine University, France.

  - Pierre-Cyrille Héam, Calculability, 23 hours (ETD), M2 Computer science, Université de Franche-Comté, France.
  - Pierre-Cyrille Héam, Introduction to Büchi Automata, 18 hours (ETD), M2 Computer science, Université de Franche-Comté, France.
  - Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, University of Lorraine, France.
  - Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2, Université de Franche-Comté, France.
  - Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2, Université de Franche-Comté, France.
  - Olga Kouchnarenko, Security and Components, 10,5 hours (ETD), M2, Université de Franche-Comté, France.
- Doctorat:
  - Steve Kremer, Les protocoles de sécurité : modélisation et vérification, 4,5 hours (ETD), École jeunes chercheurs en programmation (EJCP), Rennes, France

9.2.2. Supervision

- PhD :

  Kalou Cabrera Castillos, Automated Test Scenario Generation from Property Patterns and Behavioral Models, November 28, Frédéric Dadeau and Jacques Julliand

  Jérome Cantenot, Management of consistence in verication conditions in the test generation context, Université de Franche Comté, 13 November, Fabrice Ambert and Fabrice Bouquet.

  Vincent Hugot, Approximations and Constraints: Application to the Verification of Embedded Systems, Université de Franche Comté, September 27, Pierre-Cyrille Héam and Olga Kouchnarenko

  Elena Tushkanova, Specification and formal certification of (combinations of) decision procedures, Université de Franche Comté, July 19, Alain Giorgetti, Olga Kouchnarenko and Christophe Ringeissen
- PhD in progress :

  Hadrien Bride, Validation and Reconfiguration of Modal Petri Nets within Constraint Logic Programming, started in October 2013, Olga Kouchnarenko and Fabien Peureux

  Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune

  Aloïs Dreyfus, Efficient approches for systems validation, started in November 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

  Ivan Enderlin, Test Data Generation for Unit Testing in PHP, started in October 2011, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

  Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on microsystems, started in October 2012, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad

  Richard Genestier, Formal specification and verification of programs generating structured data, started in October 2012, Alain Giorgetti and Olga Kouchnarenko

  Bao-Thien Hoang, Secure Collaboration in Social Networks, started in April 2011, Abdessamad Imine and Christophe Ringeissen

  Jean-Luc Joly, Randomized approaches for validation and verification procedures, started in December 2011, Pierre-Cyrille Héam

  Robert Künnemann, Verification of Security APIs, started in October 2010, Steve Kremer and Graham Steel

Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, Véronique Cortier

Houari Mahfoud, Access Control Models for XML Documents, started in September 2010, Abdessamad Imine and Michaël Rusinowitch

Guillaume Scerri, Symbolic and automatic security proofs in computational models, started in September 2011, Hubert Comon-Lundh and Véronique Cortier

Cyrille Wiedling, Formal analysis of E-voting protocols, started in September 2011, Véronique Cortier

Hiep Nguyen Huu, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

9.2.3. Juries

Inria evaluation committee (Véronique Cortier, Michaël Rusinowitch)

Jury starting/advanced Inria positions and jury international chair Inria 2013 (Véronique Cortier)

Jury Junior Research Position Inria Nancy Grand Est (Michaël Rusinowitch)

Referee for David Cadé's PhD, December 2013: Proved Implementations of Cryptographic Protocols in the Computational Model (Véronique Cortier)

Referee for Matthijs Melissen's PhD, October 2013: Game Theory and Logic for Non-repudiation Protocols and Attack Analysis (Steve Kremer)

Referee for Jannik Dreier's PhD, November 2013: Formal Verification of Voting and Auction Protocols: From Privacy to Fairness and Verifiability (Steve Kremer)

Referee for Naipeng Dong's PhD, November 2013: Enforced Privacy: from Practice to Theory (Michaël Rusinowitch)

Referee for Mohamed Iguernelala's PhD, June 2013: Renforcement du Noyau d'un Démonstrateur SMT (Michaël Rusinowitch)

Referee for Sarah Nait Bahloul's PhD, December 2013: Inférence de règles de contrôle d'accès pour assurer la confidentialité des données au niveau des vues matérialisées (Michaël Rusinowitch)

Referee for Robert Guduvan's PhD, April 2013, A model driven Development of tests for avionics embedded systems (Fabrice Bouquet)

Referee for Taha Triki's PhD, October 2013, Filtering and reduction techniques combinational tests (Fabrice Bouquet)

Examiner for Florent Pompigne's PhD, December 2013, Nancy: Modélisation logique de la langue et Grammaires Catégorielles Abstraites (Laurent Vigneron).

Examiner for Asma Tafat's PhD, September 2013, Orsay: Preuves par raffinement de programmes avec pointeurs. (Alain Giorgetti).

Commitee chair for Lilia Ziand Khodja's PhD, May 2013, Besançon: Résolution de systèmes linéaires et non linéaires creux sur grappes de GPU's (Pierre-Cyrille Héam).

9.3. Popularization

Invited conference of Véronique Cortier at the conference "Sciences et Société", Nancy, January 17th, 2013.

"Vote par internet", popularization science paper on e-voting. In Interstices, January 2013. Véronique Cortier and Steve Kremer.

Fête de la Science 2013: Science popularization action during one week on a workshop "a cryptographic treasure hunting". Véronique Cortier, David Galindo, Stéphane Glondu, Steve Kremer, Éric Le Morvan, Cyrille Wiedling.

Video gaming month at the “Fabrikà Science”, University of Franche-Comté, December 2013. Popularization of computer science using the topic of video games. Frédéric Dadeau.

COMETE Project-Team

8. Dissemination

8.1. Scientific Animation

Note: In this section we include only the activities of the permanent internal members of Comète.

8.1.1. Editorial activity

Catuscia Palamidessi is/has been:

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, Elsevier Science.

Co-editor (with Franck van Breughel, Elham Kashefi and Jan Rutten) of a festschrift dedicated to Prakash Panagaden. Special issue of Lecture Notes in Computer Science.

Co-editor (with Geoffrey Smith) of the special issue of Mathematical Structures in Computer Science dedicated to Quantitative Information Flow.

Co-editor (with Mark Ryan) of the proceedings of TGC 2012, Trustworthy Global Computing. [27]

Frank D. Valencia has been:

Co-editor of the special issue of Mathematical Structures in Computer Science dedicated to the 18th International Workshop on Expressiveness in Concurrency.

Co-editor of the special issue of Mathematical Structures in Computer Science dedicated to the 17th International Workshop on Expressiveness in Concurrency.

Konstantinos Chatzikokolakis and Catuscia Palamidessi have been:

Co-editors (with Sebastian Mödersheim and Jun Pang) of the special issue of the Journal of Computer Security dedicated to selected papers of TOSCA 2011 and SecCo 2011.

8.1.2. Steering Committees

Catuscia Palamidessi is member of:

The Council of EATCS, the European Association for Theoretical Computer Science. Since 2005.

The Steering Committee of ETAPS, the European Joint Conferences on Theory and Practice of Software. Since 2006.

The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007.

The IFIP Working Group 2.2 – Formal Description of Programming Concepts. Since 2001.

The IFIP Working Group 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

Frank D. Valencia member of:

The steering committee of the International Workshop in Concurrency EXPRESS. Since 2010.

8.1.3. Invited Talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

Workshop on Logic, Language, Information and Computation. TU Darmstadt, Germany. August 2013.

Forum des jeunes mathématiciennes. ENS Lyon. Novembre 2013.

8.1.4. Organization of workshops and conferences

Catuscia Palamidessi is serving as PC co-chair (together with Erika Ábrahám) of FORTE 2014: the 34th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. Berlin, Germany, 3-6 June 2014. Co-located with DisCoTec 2014.

8.1.5. Participation in program committees

Catuscia Palamidessi is/has been a member of the program committees of the following conferences:

QEST 2014. The 11th International Conference on Quantitative Evaluation of Systems. Florence, Italy, 8-12 September 2014.

POST 2014. The 3rd Conference on Principles of Security and Trust. Grenoble, 5-13 April 2014.

TGC 2013. The 8th International Symposium on Trustworthy Global Computing. Buenos Aires, Argentina, 30-31 August 2013.

ICALP 2013 Track B. The 40th International Colloquium on Automata, Languages and Programming. Riga, Latvia, 8-12 July 2013.

CSF 2013. The 26th IEEE Computer Security Foundations Symposium. Tulane University, New Orleans, Louisiana, USA, 26-28 June 2013.

LICS 2013. The Twenty-Eighth Annual ACM/IEEE Symposium on Logic in Computer Science. Tulane University, New Orleans, Louisiana, USA, 25-28 June 2013.

FOSSACS 2013. The 16th Int.l Conf. on Foundations of Software Science and Computation Structures. (Part of ETAPS 2013.) Rome, Italy, March 2013.

SOFSEM 2013. 39th International Conference on Current Trends in Theory and Practice of Computer Science. Špindlerův Mlýn, Czech Republic, January 26–31, 2013.

Frank D. Valencia is/has been a member of the program committees of the following conferences and workshops:

CONCUR 2013. The 24th International Conference on Concurrency Theory. Buenos Aires, Argentina, 27-30 August 2013.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

ICFEM 2014: The 6th International Conference on Formal Engineering Methods.

PETS 2014: The 14th Privacy Enhancing Technologies Symposium.

HotPETs 2014: 7th Workshop on Hot Topics in Privacy Enhancing Technologies.

QAPL 2014: 12th Workshop on Quantitative Aspects of Programming Languages.

ISPEC 2013: 9th International Conference on Information Security Practice and Experience.

QAPL 2013: 11th Workshop on Quantitative Aspects of Programming Languages.

HotPETs 2013: 6th Workshop on Hot Topics in Privacy Enhancing Technologies.

8.1.6. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the Swedish Research Council Committee for Computer Science, 2013. The main duty of this committee is to evaluate and select the grant applications.

Member of the committee for the ACM SIGSAC 2014 Doctoral Dissertation Award for Outstanding PhD Thesis in Computer and Information Security.

Member of the committee for the Ackermann Award 2013: The EACSL outstanding dissertation award for logic in Computer Science.

President of the selection committee for the EATCS Best Paper Award at the ETAPS conferences. Since 2006.

Member of the EAPLS PhD Award committee. Since 2010.

8.1.7. Organization of seminars

Frank D. Valencia, Luis Fernando Pino Duque, and Nicolás Bordenabe are the organizer of the Comète-Parsifal Seminar. This seminar takes place weekly at LIX, and it is meant as a forum where the members of Comète and Parsifal present their current works and exchange ideas.

8.1.8. Service

Catuscia Palamidessi serves as:

Member of the Comité d'Orientation Scientifique et Technique, Groupe de travail Relation Internationales (COST-GTRI). Since November 2007.

Directrice adjointe du LIX, le Laboratoire d'Informatique de l'Ecole Polytechnique. Since April 2010.

Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. Since October 2007.

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master: Konstantinos Chatzikokolakis has been teaching the course "Concurrence" at the "Master Parisien de Recherche en Informatique" (MPRI) in Paris. Level M2. Total 12 hours.

Master: Frank D. Valencia has been teaching the course "Concurrence" at the "Master Parisien de Recherche en Informatique" (MPRI) in Paris. Level M2. Total 12 hours.

Master. Frank D. Valencia has been teaching an advanced course on Process Modeling at the Master Program in Computer Science of the Pontificia Universidad Javeriana de Cali, Colombia. Total 30 hours. A.Y. 2012-13.

8.2.2. Supervision

PhD (2010-2013) Sophia Knight. Ecole Polytechnique. Grant Inria/CORDIS. Title of the thesis: *The Epistemic Dimension of Concurrency Theory*. Defended on 20 Sep 2013. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD (2009-2013) Ivan Gazeau. Ecole Polytechnique. Grant ANR. Title of the thesis: *Safe Programming in finite precision: Controling the errors and information leaks*. Defended on 14 Oct 2013. Co-supervised by Catuscia Palamidessi and Dale Miller.

PhD in progress (2012-) Marco Stronati. Ecole Polytechnique. Grant EDX Monge. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-) Lili Xu. Ecole Polytechnique and Chinese academy of Science, Beijing, China. Co-supervised by Catuscia Palamidessi and Huimin Li.

PhD in progress (2011-) Nicolás E. Bordenabe. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-) Luis Fernando Pino Duque. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD in progress (2013-) Salim Percy. Ecole Polytechnique. Grant Digiteo-Digicosme. Co-supervised by Frank D. Valencia and Stefan Haar.

8.2.3. Other didactical duties

Catuscia Palamidessi is:

- Co-responsible of the Master 2 course on Concurrency since 2003, first at the DEA in Theoretical Computer Science (Paris) and then at the MPRI.
- External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.
- Member of the advising committee for the PhD of Andrea Margheri, University of Florence, Italy.

DICE Team

9. Dissemination

9.1. Scientific Animation

The digital revolution induces rapid changes in our societies, that are often not well prepared to adapt and take full advantage of them. Our objective is to communicate broadly to non specialist communities, through teaching, conferences in other communities, as well as through the media.

S Frénot and/or S Grumbach have been invited speaker or panelist at the following conferences in IT related fields:

- Panel La politique des données personnelles : big data ou contrôle individuel ?, IXXI, ENS de Lyon et Villa Gillet (Festival Mode d'Emploi), Lyon, 21 novembre 2013.
- Chair and organization of Session Managing the flow computing, Fossa, Lille, novembre 2013. Slides and presentation for this session are available at https://fossa.inria.fr/slides/
- Tutoriel Les flux de données personnelles, enjeux technologiques, économiques et stratégiques, 29e Journées Bases de Données Avancées, Nantes, 22-25 Octobre 2013.
- Panel: Big Data : c'est aussi un sujet de sécurité, Les assises de la sécurité et des systèmes d'information, Monaco, 2-5 octobre 2013.
- Invited speaker Congrès Big Data, Turning the Data Deluge into Decisions, CNIT, Paris, avril 2013
- La France à la périphérie de la société de l'information? Café techno, Paris, mars 2013
- Panel on Big Data, 6th International Conference on Computers, Privacy and Data Protection, CPDP, Reloading Data Protection, Brussels, january 2013

9.2. Teaching - Supervision - Juries

Teaching

We have been involved in the following courses:

- INSA, Frénot, Grumbach, TweetMyFace: A 38 hours optional course on social network technical architectures, evolutions and designs. The course covers current Web technologies from low-level networking to Facebook and Twitter API. L2 (Since 2012)
- INSA, Frénot, Agility: A 32 hours optional course on agile software development presenting both iterative (SCRUM) and stream based approaches (LEAN IT). M1. (since 2011)
- INSA, Frénot, Innovating Project: Supervising 250 hours student project aim at managing innovating projects. Each student group leads its own subject during one semester. All projects and organizational details are publicly available here: http://tc-pi.insa-lyon.fr M1 (Since 2006)
- INSA, Frénot, Learn Other Languages: The aim of the course is to improve one's skills in current state-of-the-art programing and discover different ways to develop using mainly web-oriented programming languages. M1 (new course)
- INSA, Frénot, Innovation and Transfer for Software: This final year optional course targets a specific activity for engineer profession dedicated to software transfert from research labs to industrials.

Stéphane Grumbach supervised the following thesis:

PhD: Ahmad Ahmad-Kassem, Programming Networks with Intentional Destination, Université de Lyon, november 2013

Stéphane Frénot supervised the following thesis:

- Etienne Brodu started in 2013. Worldline partnership CIFRE Phd. "Flow-base operating systems and programing languages. A new deal for social network architectures"
- François Goichon defense december 2013. French Ministry of research. "Resource access equity for best-effort shared operating systems"
- Zheng Hu defense january 2014. Orange-Labs partnership CIFRE PhD. "Self-configuration, monitoring and control of physical entities via Sensor and Actuator Networks"
- Dan Yufang defense Mid 2014. CSC China. "Secure and healable usage of components in a dynamic service-oriented architecture-based system"
- Manuel Selva defense End 2014. Bull SA partnership. "Monitoring data-flow programs"

Juries

Stéphane Frénot was involved in the following committee as reporting member.

- Roberto Minerva: Will the telco survive to an ever changing world? Technical considerations leading to disruptive scenarios.
- Aurelien Faravelon: A privacy aware conceptual and implementation framework for service oriented architecture based on access control.
- Azzedine Amiar : Trace and log analysis in micro-controllers.

9.3. Popularization

Intervention in other arenas:

- Co-organization of the CARA community, that gather IT professionals around agility design. Meetings occurs once per month from 7PM to 10PM and gather around 50 people to discuss and debate. The complete animation scheme is available at http://lyon.clubagilerhonealpes.org/
- La révolution numérique, L'enseignement philosophique et les sciences: nouvelles perspectives, Fondation Simone et Cino del Duca, Paris, 13 novembre 2013
- Panel: Open Data and Civic Participation, Can "Open Data" Improve Democratic Governance?, CITRIS Data & Democracy Initiative and Institute of Governmental Studies, Berkeley, 12 September 2013.
- Big Data: Where Does Europe Stand? a Citizen's Controversy, at the Madariaga – College of Europe Foundation, with Roberto Viola, Deputy Director of DG Communication, Brussels, 12 July 2013.
- La Révolution numérique, un enjeu politique, Conférence au Cercle Pierre Mendes France de Lyon, 25 juin 2013
- Les données, nouveau moteur de l'économie, Congrès France Génétique Elevage, janvier 2013

Intervention in political instances. The Dice team aims at interacting with political representatives at the French Assemblée nationale, the Sénat, as well as instances of the European Union.

- Global perspective on the information society, Invited speaker at the Council of the European Union, Part I Europe at the periphery of the information society? Brussels, April 17, 2013,
  Part II Information society in China, the Beijing consensus? Brussels, May 14, 2013,
- La dépendance de la France en matière de données et services numériques, Assemblée Nationale, Audition publique du 21 février 2013, "Le risque numérique : en prendre conscience pour mieux le maîtriser ?",

PRIVATICS Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Organization

Claude Castelluccia : WISEC 2014.

Mathieu Cunche : WISEC 2014.

Cédric Lauradoux : Colloque CAPPRIS-AFDIT, 11/09/2013, Lyon, http://planete.inrialpes.fr/capprisafdit.

Daniel Le Métayer : Colloque CAPPRIS-AFDIT, 11/09/2013, Lyon, http://planete.inrialpes.fr/capprisafdit.

Vincent Roca : SAR-SSI 2014.

8.1.2. Program committee

Claude Castelluccia : PETS 2013, WISEC 2013, POST 2013, SESOC 2013.

Mathieu Cunche : WCNC 2014.

Cédric Lauradoux : ACNS 2013, Cardis 2013, GreHack 2013, WISEC 2014.

Daniel Le Métayer : CPDP 2013, APF 2013, APVP 2013, WOSSAP 2013, SAR-SSI 2013.

Vincent Roca : SPACOMM 2014, SNDS 2014, SSCC 2013.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Undergraduate course : Vincent Roca, On Wireless Communications, 12h, L1, Polytech' Grenoble, France.

Undergraduate course : Vincent Roca, On Network Communications (24h), L1, IUT-2 (UPMF University) Grenoble, France.

Undergraduate course : Marine Minier, Probabilities, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Signal Processing, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Analysis, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Introduction to Cryptography, 30h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Information Theory, 30h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Micromachine, 20h, L3, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, Introduction to computer science, 120h, L1, INSA-Lyon, France.

Master : Claude Castelluccia, Wireless Security, 20h, M2, Ensimag/University of Grenoble, France.

Master : Claude Castelluccia, Wireless Security, 15h, M2, Ensimag/INPG, France.

Master : Marine Minier, Security for wireless networks, 10h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, Wireless Security, 2h, M2, INSA-Lyon, France.

8.2.2. Supervision

PhD in progress : Jagdish Achara, Mobile devices and operating systems from a privacy point of view, October 2013, Vincent Roca and Claude Castelluccia.

PhD in progress : Thibaud Antignac, New solutions for a better privacy, September 2011, Daniel Le Métayer.

PhD in progress : Abdelberi Chaabane, Threats against privacy on Internet: evaluation and solutions, September 2010, Mohamed Ali Kaafar and Claude Castelluccia.

PhD in progress : Jessye Dos Santos, Wireless physical tracking, October 2013, Cédric Lauradoux and Claude Castelluccia.

PhD in progress : Amrit Kumar, Privacy and multiparty computation, November 2013, Cédric Lauradoux.

PhD in progress : Ferdaouss Mattoussi, Design and optimizations of AL-FEC: GLDPC-Staircase Codes, September 2010, Vincent Roca and Claude Castelluccia.

PhD in progress : Lukasz Olejnik, Internet Tracking and Profiling, October 2011, Claude Castelluccia.

PhD in progress : Vincent Primault, Privacy and geolocated services, November 2013, Cédric Lauradoux.

PhD in progress : Gael Thomas, Algebraic Automata in Symetric Cryptography, November 2011, Marine Minier.

PhD in progress : Minh-Dung Tran, Privacy-Preserving Ad systems, September 2011, Claude Castelluccia and Mohamed Ali Kaafar.

PhD in progress : Dong Wang, titre (provisoire) du mémoire, date du début de la thèse, Mohamed Ali Kaafar.

8.2.3. Juries

HdR : Marc-Olivier Killijian, Towards Resilient and Private Mobiquitous Systems, Toulouse, 20/02/2013, Claude Castelluccia.

PhD : Ahmed Benfarah, Security of a UWB-IR link, INSA-Lyon, 10/07/2013, Cédric Lauradoux.

PhD : Ludovic Jacquin, Efficiency/Security trade-off for High Bandwidth Internet Gateway, Grenoble, 20/11/2013, Vincent Roca and Claude Castelluccia.

PhD : Mohammad Nabil ALAGGAN, Private Peer-to-peer similarity computation in personalized collaborative platforms, Rennes, 16/12/2013, Daniel Le Métayer.

PhD : Sophie Guicherd, Le régime juridique applicable aux dysfonctionnements du logiciel, 05/12/2013, Daniel Le Métayer.

8.3. Popularization

Claude Castelluccia and Daniel Le Métayer, La vie privée, un obstacle à l'économie numérique ?, LeMonde.fr, 03.09.2013, http://www.lemonde.fr/economie/article/2013/08/25/la-vie-privee-un-obstacle-a-l-economie-numerique_3466139_3234.html.

Mathieu Cunche, Smartphone, Wi-Fi et vie privée : comment votre smartphone peut se révéler être votre pire ennemi [35], October 2013, MISCMAG.

Mathieu Cunche, Quand les terminaux mobiles jouent les mouchards de poche, Podcast Interstices, September 2013, https://interstices.info/jcms/ni_74624/quand-les-terminaux-mobiles-jouent-les-mouchards-de-poche.

Cédric Lauradoux and Levent Demir, Guesswork [40], October 2013, MISCMAG.

Mobilitics project, Paris Metro Tracks and Trackers: Why is the RATP App leaking my private data?

Mobilitics project, Voyage au cœur des smartphones et des applications mobiles avec la CNIL et Inria, 09/04/2013, bit.ly/M3cWCi.

PROSECCO Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Journal Editorial Boards

Associate Editor

– of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: Bruno Blanchet

9.1.2. Conference Program Committees

- FCS – June 2013, New Orleans, LA, USA: Bruno Blanchet (PC co-chair)
- POST – April 2014, Grenoble, France: Bruno Blanchet
- SEC@SAC – March 2013, Coimbra, Portugal: Graham Steel (PC co-chair)
- CSF – June 2013, New Orleans, USA: Graham Steel
- IWIL – December 2013, Stellenbosch, South Africa: Graham Steel

9.1.3. Participation to Workshops and Conferences

ETAPS – March 2013, Rome, Italy: Bruno Blanchet, David Cadé, Miriam Paiola, Benjamin Smyth

CSF, FCS, FCC – June 2013, New Orleans, LA, USA: Bruno Blanchet, Benjamin Smyth

CCS – November 2013, Berlin, Germany: Bruno Blanchet, David Cadé, Miriam Paiola, Gergely Bana

S&P – May 2013, San Francisco, USA: Karthikeyan Bhargavan, Alfredo Pironti

Usenix Security, WOOT – August 2013, Washington DC, USA: Karthikeyan Bhargavan, Alfredo Pironti, Antoine Delignat-Lavaud

CryptoForma – September 2013, San Francisco, USA: Alfredo Pironti

Black Hat USA – July 2013, Las Vegas, USA: Benjamin Smyth

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII, France

Karthikeyan Bhargavan, TDs in INF431 and INF321, introductory programming language courses at Ecole Polytechnique, France

Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII, France

Bruno Blanchet, Automatic Verification of Cryptographic Protocols in the Symbolic Model, the Automatic Verifier ProVerif, 6h equivalent TD, 13th International School on Foundations of Security Analysis and Design (FOSAD'13), Bertinoro, Italy

Miriam Paiola, Internet et Outils - IO2, TP, 52h equivalent TD, L1 en Math-Info, Université Paris VII, France

Miriam Paiola, Automates finis - AF4, TP, 26h equivalent TD, L2 en Informatique, Université Paris VII, France

Graham Steel, Formal Methods for the Science of Security Summer School, UIUC, July 2013, "Security APIs" (4 hours teaching)

Graham Steel, SecAppDev Days Training, Katholieke Universiteit Leuven, March 2013, "Security APIs" (3 hours teaching)

Graham Steel, University of Venice Ca' Foscari, PhD course "Security APIs" October/November 2013, (20 hours teaching)

Evmorfia-Iro Bartzia, Introduction to Mathematical Cryptography (cours + TD), MACS3: Mathématiques appliquées et calcul scientifique 3eme année, Université Paris 13

Evmorfia-Iro Bartzia, Elliptic Curves and Complex Torus (TD), MFPI: Mathématiques Fondamentales et Protection de l'Information, Université Paris 8

9.2.2. Supervision

- David Cadé
  Proved Implementations of Cryptographic Protocols in the Computational Model,
  defended on December 16, 2013, supervised by Bruno Blanchet
- Miriam Paiola
  Automatic Verification of Group Protocols,
  since November 2010, supervised by Bruno Blanchet
- Robert Künnemann, *Secure APIs and Simulation-Based Security*, Started Oct. 2010, supervised by Steve Kremer (CASSIS) and Graham Steel, submitted October 2013 will defend January 2014
- Gavin Keighren, *A Type System for Security APIs*, since 2007 (submitted August 2013), advisors Graham Steel and David Aspinall (University of Edinburgh). Will defend January 2014.
- Antoine Delignat-Lavaud, since 2012, supervised by Karthikeyan Bhargavan
- Evmorfia-Iro Bartzia, since 2011, supervised by Karthikeyan Bhargavan and Pierre-Yves Strub

9.2.3. Internships

- Benjamin Beurdouche did an undergraduate internship under the supervision of Alfredo Pironti and Karthikeyan Bhargavan
- Adam McCarthy did a masters internship under the supervision of Benjamin Smyth

9.2.4. Juries

- Jannik Dreier – Ph.D. – Nov. 25, 2013 – Université de Grenoble
  Bruno Blanchet
- Maria Christofy – Ph.D. –Feb. 15, 2013– UVSQ
  Graham Steel (rapporteur)
- François Dupressoir – Ph.D.–Feb. 6, 2013– Open University
  Graham Steel (rapporteur)

9.3. Popularization

9.3.1. Vulnerability Reports

- Benjamin Smyth and Alfredo Pironti reported TLS truncation vulnerabilities to Helios, Microsoft, and Google, and presented a talk at BlackHat USA. They were acknowledged in Google's Hall of Fame.
- Karthikeyan Bhargavan and Antoine Delignat-Lavaud reported HTTPS header truncation vulnerabilities in Google Chrome and Apple Safari, resulting in a security update to Google Chrome.
- Karthikeyan Bhargavan and Antoine Delignat-Lavaud reported TLS protocol-level vulnerabilities in Internet Explorer, Google Chrome, and Mozilla Firefox, resulting in security updates to all three.
- Antoine Delignat-Lavaud reported new vulnerabilites in Akamai-hosted websites, resulting in an update to Akamai's web caching network.