



RESEARCH CENTER

FIELD

Algorithmics, Programming, Software and Architecture

Activity Report 2014

Section Dissemination

Edition: 2015-03-24

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

1. ARIC Project-Team	5
2. CAMEL Project-Team	9
3. CASCADE Project-Team	14
4. CRYPT Team	18
5. GALAAD2 Team	20
6. GEOMETRICA Project-Team	23
7. GRACE Project-Team	27
8. LFANT Project-Team	31
9. POLSYS Project-Team	34
10. SECRET Project-Team	38
11. SPECFUN Project-Team	42
12. VEGAS Project-Team	44

ARCHITECTURE, LANGUAGES AND COMPILATION

13. ALF Project-Team	47
14. ATEAMS Project-Team	49
15. CAIRN Project-Team	51
16. CAMUS Team	56
17. COMPSYS Project-Team	59
18. DREAMPAL Team	62
19. GCG Team	65
20. PAREO Project-Team	66
21. POSTALE Team	69
22. TASC Project-Team	71

EMBEDDED AND REAL-TIME SYSTEMS

23. AOSTE Project-Team	76
24. CONVECS Project-Team	79
25. HYCOMES Team	84
26. MUTANT Project-Team	85
27. PARKAS Project-Team	87
28. SPADES Team	89
29. TEA Project-Team	91

PROOFS AND VERIFICATION

30. ANTIQUE Team	92
31. CELTIQUE Project-Team	98
32. DEDUCTEAM Exploratory Action	102
33. ESTASYS Exploratory Action	105
34. GALLIUM Project-Team	106
35. MARELLE Project-Team	109
36. MEXICO Project-Team	111
37. PARSIFAL Project-Team	113

38. PIR2 Project-Team	116
39. SUMO Project-Team	121
40. TEMPO Team	124
41. TOCCATA Project-Team	125
42. VERIDIS Project-Team	131
SECURITY AND CONFIDENTIALITY	
43. CARTE Project-Team	134
44. CASSIS Project-Team	137
45. COMETE Project-Team	141
46. DICE Team	146
47. PRIVATICS Project-Team	149
48. PROSECCO Project-Team	153

ARIC Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific animation

- Guillaume Hanrot is director of the LIP laboratory (Laboratoire de l'Informatique du Parallélisme) since April 1, 2014. He was deputy director of the LIP before;
- Jean-Michel Muller is co-director of the Groupement de Recherche (GDR) *Informatique Mathématique* of CNRS;
- Gilles Villard has been director of the LIP laboratory until April 1, 2014.

9.1.2. Scientific events organisation

9.1.2.1. general chair, scientific chair

Damien Stehlé is a member of the steering committee of the PQCrypto conference series. He is also a member of the steering committee of the Cryptography and Coding French research grouping (C2).

Claude-Pierre Jeannerod is a member of the scientific committee of JNCF (Journées Nationales de Calcul Formel).

9.1.2.2. member of the organizing committee

Bruno Salvy was one of the organizers of a workshop “Challenges in 21st Century Experimental Mathematical Computation”, at ICERM, Providence, Rhode Island.

Nicolas Brisebarre and Jean-Michel Muller organized a one week workshop “Formal Proof, Symbolic Computation and Computer Arithmetic” which took place from February 3 to February 7 (50 participants), in the framework of a whole month devoted to “Mathematical Structures of Computation” in Lyon.

9.1.3. Scientific events selection

9.1.3.1. member of the conference program committee

Jean-Michel Muller was a member of the program committees of ASAP'2014 and ARITH'2015.

Damien Stehlé was a member of the program committees of LATINCRYPT'14, PQCrypto'14, and ACISP'14.

Bruno Salvy was a member of the program committee of AofA'2014.

Fabien Laguillaumie was a member of the program committee of Africacrypt'14.

Benoît Libert was a member of the program committee of ACM-CCS'14.

9.1.4. Journal

9.1.4.1. member of the editorial board

- Jean-Michel Muller is a member of the editorial board of the *IEEE Transactions on Computers*. He is a member of the board of foundation editors of the *Journal for Universal Computer Science*. He was co-guest editor of a special issue of the journal *Science of Computer Programming* [32].
- 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).
- Gilles Villard is a member of the editorial board of the *Journal of Symbolic Computation*.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

Master: Nicolas Brisebarre, *Introduction to Effective Approximation Theory* (24h), Hanoi Institute of Mathematics (Vietnam).

Master: Claude-Pierre Jeannerod, Nicolas Louvet, Nathalie Revol, *Algorithmique numérique et fiabilité des calculs en arithmétique flottante* (24h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Master: Vincent Lefèvre, *Arithmétique des ordinateurs* (20h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Professional teaching: Nathalie Revol, *Contrôler et améliorer la qualité numérique d'un code de calcul industriel* (2h30), Collège de Polytechnique.

Master: Fabien Laguillaumie, *Cryptography, Error Correcting Codes*, 150h, Université Claude Bernard Lyon 1.

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

Master: Benoît Libert, *Advances cryptographic protocols*, 24h, ENS de Lyon.

Research school: Adeline Langlois, Fabien Laguillaumie, Damien Stehlé, *Chiffrement avancé à partir du problème Learning With Errors* (4h30), École de printemps Codes et Crypto, Université de Grenoble.

Research school: Adeline Langlois, Fabien Laguillaumie, Damien Stehlé, *Chiffrement avancé à partir du problème Learning With Errors* (4h30), École Jeunes Chercheurs en Informatique Mathématique, Université de Caen.

Research school: Damien Stehlé, *Cryptographie reposant sur les réseaux euclidiens* (3h), Colloque Jeunes Chercheurs en Théorie des Nombres.

9.2.2. Supervision

PhD : Nicolas Brunie, *Contribution à l'arithmétique des ordinateurs et applications aux systèmes embarqués*, ENS Lyon, May 2014, co-supervised by Florent de Dinechin (and Renaud Ayrignac).

PhD : Adeline Langlois, *Lattice - Based Cryptography - Security Foundations and Constructions*, ENS Lyon, October 2014, supervised by Damien Stehlé.

PhD : Philippe Théveny, *Numerical quality and high performance in interval linear algebra on multi-core Processors*, ENS Lyon, October 2014, supervised by Nathalie Revol.

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

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 : Antoine Plet, *Contribution à l'analyse d'algorithmes en arithmétique virgule flottante*, since September 2014, co-supervised by Nicolas Louvet and Jean-Michel Muller.

PhD in progress : Valentina Popescu, *Vers des bibliothèques multi-précision certifiées et performantes*, since September 2014, co-supervised by Mioara Joldes (LAAS) and Jean-Michel Muller.

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.

PhD in progress: Louis Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, co-supervised by Alin Bostan (SpecFun team) and Bruno Salvy.

PhD in progress: Sébastien Maulat, *Évaluation efficace et certifiée de fonctions différentiellement finies en précision modérée*, since september 2014, supervised by Bruno Salvy.

PhD in progress: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.

9.2.3. Juries

In 2014, Jean-Michel Muller was vice-chair of the “Comité d’évaluation scientifique mathématiques–informatique théorique” of the ANR (the French national research agency). He participated to the PhD committees for the defenses of Laurent Thévenoux (Univ. Perpignan) and Karim Bigou (Univ. Rennes 1). He participated to the Habilitation committees for the defenses of Christophe Denis (Univ. Perpignan), Sylvie Boldo (Paris Sud Univ.) and David Defour (Univ. Perpignan). He was a member of the Scientific Council of ENS de Lyon until june 2014, and he is a member of the Scientific Council of CERFACS (Toulouse).

Bruno Salvy was a member of the PhD committees of Julien Courtien (Bordeaux), Jules Svartz (UPMC), and Pierre Lairez (École polytechnique).

Nathalie Revol was a member of the PhD committee of Olivier Mullier (École polytechnique). Nathalie Revol was in the hiring committee for junior researchers (CR) of Inria Grenoble - Rhône-Alpes and in the hiring committee for an assistant professor position at Université Paris Sud.

Damien Stehlé was reviewer of the PhD theses of Robert Fitzpatrick (Royal Holloway, UK), Tancred Lepoint (ENS Paris, Univ. du Luxembourg and CryptoExperts) and Nicola di Pietro (Univ. Bordeaux).

Fabien Laguillaumie was reviewer for the PhD thesis of Alain Patey (Telecom ParisTech). He was part of the HDR committee of Damien Vergnaud (ENS).

Nicolas Louvet was a member of a hiring committee for an associate professor position at the university Montpellier 2.

9.3. Invited Conferences

- Damien Stehlé gave an invited talk *Secure lattice codes for the gaussian wiretap channel*, at the Algebra, Codes and Networks symposium, Bordeaux, France, in June 2014;
- Damien Stehlé gave an invited talk *The Learning with Errors problem*, at the Oberwolfach workshop on combinatorial optimization, Oberwolfach, Germany, in November 2014;
- Jean-Michel Muller gave two invited talks, *On the maximum relative error when computing x^n in floating-point arithmetic* (in Tokyo) and *On complex multiplication and division with an FMA* (in Kyoto), for the conference INVA 2014, Japan, in March 2014;
- Jean-Michel Muller gave an invited talk *Getting tight error bounds in floating-point arithmetic: illustration with complex functions, and the real x^n function*, at the workshop *NSV’2014: Numerical Software Verification*, Vienna, in July 2014.
- Bruno Salvy gave an invited talk *Algorithmic variations on linear differential equations* at the MBM2014 day organized in Bordeaux in October when Mireille Bousquet-Mélou received the silver medal of the CNRS. He was also invited to give a talk in Oberwolfach, for their meeting on Enumerative Combinatorics in March, where he talked about *Multiple Binomial Sums*, of which he had given a previous version in February at the “Holonomy days” where he had been invited in Grenoble.

- Nathalie Revol gave invited talks at the workshop “Challenges in 21st Century Experimental Mathematical Computation” at ICERM, Providence, Rhode Island, and at French seminars: CEA-LIST, Inria comité des projets, Aristote.
- Fabien Laguillaumie gave an invited scientific committee talk *Anonymity-oriented Signatures based on Lattices* at the YACC’14 conference, Porquerolles, France, in June 2014.

9.4. Popularization

- Sylvie Boldo (Proval project) and Jean-Michel Muller wrote a popular science paper *Des ordinateurs capables de calculer plus juste* in the journal *La Recherche* [36].
- Nicolas Brisebarre co-organizes scientific conferences, called «Éclats de sciences», at Maison du Livre, de l’Image et du Son in Villeurbanne. Around three conferences take place per year.
- Nathalie Revol gave talks for pupils at collèges and lycées, as an incentive to choose scientific careers: lycée Camille Vernet (Valence, Drôme), lycée Jérémie de la Ville (Charlieu, Loire), lycée Gabriel Fauré (Annecy, Haute-Savoie), collège Jean Renoir (Neuville-sur-Saône, Rhône). During the “Week of mathematics”, she gave a 2-hour talk at lycée de la Côtière (La Boisse, Ain). She gave the inaugural conference of the congress “Math en Jean’s” in Lyon and the conference for the scientific camp “Math C2+” in Montbonnot. She was present for the “Mondial des Métiers” (Eurexpo Lyon, Chassieu, Rhône). For the Science Fair, she gave 2 talks at MMI, ENS de Lyon. In 2014, she met over 1000 pupils.

CAMEL Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Steering committee membership

- Pierrick Gaudry is a member of the steering committee of the ECC (Elliptic Curve Cryptography) conference series.
- Emmanuel Thomé is a member of the steering committee of the ANTS (Algorithmic Number Theory Symposium) conference series (which gathers the program committee chairs and proceedings editors of previous conference editions).

9.1.2. Scientific events selection

9.1.2.1. Conference program committee chairing

- Jérémie Detrey was program chair for the poster session of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014).

9.1.2.2. Conference program committee membership

- Jérémie Detrey was a member of the program committee of
 - the architecture track of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014),
 - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014).
- Pierrick Gaudry was a member of the program committee of
 - the 18th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2015),
 - the 5th International Workshop on the Arithmetic of Finite Fields (WAIFI 2014).
- Emmanuel Thomé was a member of the program committee of
 - Selected Areas in Cryptography (SAC 2014),
 - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014).
- Marion Videau was a member of the program committee of
 - Selected Areas in Cryptography (SAC 2014),
 - the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014),
 - the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2014).

9.1.2.3. Reviewing activities

- Jérémie Detrey reviewed submissions to
 - the architecture track of the *Conférence en Parallélisme, Architecture et Système* (ComPAS 2014),
 - Selected Areas in Cryptography (SAC 2014),

- the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014),
- the 16th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2014),
- the 6th International Conference on Post-Quantum Cryptography (PQCrypto 2014).
- Pierre-Jean Spaenlehauer reviewed submissions to
 - the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014),
 - Symbolic-Numeric Computation (SNC 2014).
- Hugo Labrande reviewed submissions to
 - Selected Areas in Cryptography (SAC 2014).
- Pierrick Gaudry reviewed submissions to
 - the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2014),
 - the 12th International Conference on Applied Cryptography and Network Security (ACNS 2014).
- Emmanuel Thomé reviewed submissions to
 - Selected Areas in Cryptography (SAC 2014),
 - the Third International Conference on Cryptology and Information Security in Latin America (Latincrypt 2014),
 - the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2014),
 - the 34rd International Cryptology Conference (Crypto 2014),
 - the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014).
- Marion Videau reviewed submissions to
 - Selected Areas in Cryptography (SAC 2014),
 - the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014),
 - the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2014).

9.1.3. Journal activities

9.1.3.1. Editorial board membership

- Pierrick Gaudry is an editor of the journal *Applicable Algebra in Engineering, Communication and Computing*.

9.1.3.2. Reviewing activities

- Jérémie Detrey reviewed submissions to
 - the IEEE Transactions on Computers (IEEE TC),
 - the Journal of Cryptographic Engineering (JCEN),
 - the ACM Transactions on Mathematical Software (TOMS).
- Pierre-Jean Spaenlehauer reviewed submissions to *Designs, Codes and Cryptography*.
- Paul Zimmermann reviewed submissions to *Mathematics of Computation*, and declined several reviews for open-access and hybrid journals.
- Pierrick Gaudry reviewed submissions to *Finite field and their applications* and *Mathematics of Computation*.

- Emmanuel Thomé reviewed submissions to Designs, Codes, and Cryptography and Security and Communication Networks.

9.1.4. Invited Conferences

- Pierrick Gaudry gave invited talks at
 - the DLP 2014 workshop, in Ascona (Switzerland, May);
 - the SAC 2014 conference, in Montreal (Canada, August);
 - the *Journées nationales du calcul formel 2014*, in Marseilles (November).
- Emmanuel Thomé gave invited talks at
 - the ECC 2014 conference, in Chennai (India, October);
 - the *Journées nationales du GDR IM 2014*, in Paris (January);
 - the *École de printemps Codage et Cryptographie 2014*, in Grenoble (March);
 - the *Journées de Sécurité des Systèmes d'information*, in Rouen (November).
- Pierre-Jean Spaenlehauer gave invited talks at
 - the *Journées nationales Codage et Cryptographie 2014*, in Les Sept Laux (March);
 - the conference on Effective Moduli Spaces and Applications to Cryptology, in Rennes (June).

9.1.5. Other committees

- Pierrick Gaudry was a member of
 - the hiring committees for *chargé de recherche* positions in INRIA Nancy – Grand Est, and associate professor positions in Univ. Lorraine and Univ. Montpellier 2.
- Marion Videau was a member of
 - the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
 - the scientific committee of the *Journées Codage et Cryptographie* of GT-C2 of GdR-IM,
 - the LORIA laboratory council (elected),
 - the *Commission des développements technologiques* (CDT) of the INRIA Nancy – Grand Est research center,
 - hiring committee for an associate professor position in Univ. Lorraine,
 - hiring committee for temporary teaching and research attaché (ATER) positions in Univ. Lorraine,
 - hiring committee for teaching contracts for PhD students (DCCE) in Univ. Lorraine,
 - admission committee for student applications for a master degree in informatics in Nancy.
- Paul Zimmermann was a member of
 - the *jury d'admissibilité* for *chargé de recherche 1e classe* and *directeur de recherche 2e classe* positions at Inria, and the *jury d'admission* for *directeur de recherche 2e classe* positions at Inria.

9.1.6. Seminar organization

9.1.6.1. Caramel seminar

Ten speakers were invited to our seminar in 2014: Armand Lachand, Pierre-Jean Spaenlehauer, Guillaume Moroz, Irene Márquez-Corbella, Nicholas Coxon, Christian Eder, Andrea Miele, Thomas Richard, Enea Milio, and Sebastian Kochinke.

9.1.6.2. 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. Fourteen speakers were invited during 2014: Éric Leblond, Philippe Biondi, Eric Jaeger, Pierre-Michel Ricordel, Pascal Urien, Jérôme François, Thomas Voegtlin, Mathieu Cunche, Sébastien Bardin, Gwendall Legrand, Pierrick Gaudry, Sylvain Ruhault, Aline Gouget, and Raphaël Rigo.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

Jérémie Detrey, Security of websites, 2 hours, L1, IUT Charlemagne, Nancy, France.

Marion Videau, Introduction to algorithmic and programming, 16 hours, L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Programming methodology in C, 21 hours (lectures and tutorial sessions), L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to cryptology and information security, 20 hours (lectures and tutorial sessions), L3, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, student supervisor (for about 12 L1 students): 12 hours, L1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master:

Marion Videau and Pierrick Gaudry, Supervision of two M1 students for their *Introduction to research* practical course throughout one semester, M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to cryptology, 12 hours (lectures), M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Introduction to information system security, 24 hours (lectures and tutorial sessions), M1, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Information system security, 12 hours (lectures and tutorial sessions) and responsibility of coordinating with security seminars, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, Information system security, 21 hours+21 hours (lectures and tutorial sessions), M2, Faculté des sciences et technologies agreement with IGA, Maroc.

Marion Videau, Software validation, verification and certification: 4 hours (tutorial sessions) and responsibility of coordinating external teachers from industry.

Marion Videau and Stéphane Glondu, Supervision of the semester applied project for all M2 students from *parcours Sécurité des Architectures Web*, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, local supervision of M2 students engineering internships in industry, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Marion Videau, head of *parcours Sécurité des Architectures Web*, M2, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Misc.:

Marion Videau, teaching supervisor (*tuteur*), of a PhD student with a teaching contract (DCCE), Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

9.2.2. Internships

- David Lucas, Télécom Nancy, “Problème du rang bilinéaire : calcul et recherche de formules optimales”, Apr–Sep 2014, supervised by Jérémie Detrey.
- Théo Karaboghossian, École Normale Supérieure de Cachan, “Nombres premiers à faiblesse cachée pour le problème du logarithme discret”, Jun–Jul 2014, supervised by Pierrick Gaudry.

9.2.3. Supervision

PhD in progress:

Cyril Bouvier, Algorithmes pour la factorisation d’entiers et le calcul de logarithme discret, since Sep 2012, Paul Zimmermann.

Svyatoslav Covanov, Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides, since Sep 2014, Jérémie Detrey & Emmanuel Thomé.

Laurent Grémy, Analyse et optimisation d’algorithmes de cribles arithmétiques, since Oct 2013, Pierrick Gaudry & Marion Videau.

Hamza Jeljeli, Accélérateurs logiciels et matériels pour l’algèbre linéaire creuse sur les corps finis, since Oct 2011, Emmanuel Thomé.

Hugo Labrande, Calcul effectif d’isogénies entre jacobiniennes de courbes algébriques par une méthode d’analyse complexe, since Sep 2013, Emmanuel Thomé & Michael J. Jacobson, Jr. (Univ. Calgary, Canada).

9.2.4. Juries

- Jérémie Detrey was a member of the jury of the ÉNS competitive entrance exam.
- Paul Zimmermann was reviewer and member of the jury for the PhD thesis of Fredrik Johansson (RISC, Linz).
- Pierre-Jean Spaenlehauer was a member of the jury for the PhD thesis of Jules Svartz (EPI POLSYS, Paris).
- Pierrick Gaudry was a reviewer of the PhD thesis of Christophe Tran (Univ. Rennes 1), and a member of the jury for the PhD thesis of Ivan Boyer (Univ. Paris 7).

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”, where Paul Zimmermann gave a presentation of the Sage computer algebra system.
- Paul Zimmermann animated a “Maths-en-Jeans” group with students from the “collège” Pierre Brossolette in Réhon.
- Pierrick Gaudry gave a presentation at the “journée de l’Association francophone des spécialistes de l’investigation numérique”.
- Marion Videau
 - participated to events on information about university studies for pupils and students (Cap sur l’enseignement supérieur, Portes ouvertes de la faculté des sciences, Oriaction), and about university studies and research to the general public (Sciences en marche),
 - gave a presentation at the “journée de l’Association francophone des spécialistes de l’investigation numérique”.

CASCADE Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Organisation

7.1.1.1. Organisation of Events

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

7.1.1.2. 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 (chair)
- steering committee of PAIRING: Michel Abdalla

7.1.1.3. Board of International Organisations

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

7.1.2. Scientific Events Selection

7.1.2.1. Program Committee Chair

- Africacrypt – 28-30 May (Marrakesh, Morocco): David Pointcheval, Damien Vergnaud
- WISTP – 30 June-2 July (Heraklion, Greece): David Naccache
- SCN – 3-5 September (Amalfi, Italy): Michel Abdalla

7.1.2.2. Program Committee Member

- CS2 – 20 January (Amsterdam, Netherlands): David Naccache
- WAHC – 7 March (Rockley, Christ Church, Barbados, West Indies): David Naccache
- PKC – 26-28 March (Buenos Aires, Argentina): Michel Abdalla, Vadim Lyubashevsky
- POST – 5-13 April (Grenoble, France): David Pointcheval
- HOST – 6-7 May (Austin, TX, USA): David Naccache
- ECSaR – 27-31 May (Stanford, USA): David Naccache
- ASIACCS – 3-6 June (Kyoto, Japan): David Naccache
- HASP – 15 June (Minneapolis, MN, USA): David Naccache
- WISTP – 30 June-2 July (Heraklion, Greece): David Pointcheval
- NFSP – 3 July (Madrid, Spain): David Naccache
- IWSEC – 27-29 August (Hirosaki, Japan): Damien Vergnaud
- SCN – 3-5 September (Amalfi, Italy): Damien Vergnaud
- ESORICS – 7-11 September (Wroclaw, Poland): David Naccache
- LATINCRYPT – 17-19 September (Florianopolis, Brazil): Michel Abdalla
- ICDF2C – 18-20 September (Seoul, South Korea): David Naccache
- PQC – 1-3 October (Waterloo, Canada): Vadim Lyubashevsky

- SPACE – 18-22 October (Pune, India): David Naccache
- CANS – 22-24 October (Heraklion, Greece): Itai Dinur
- WNCS – 7-9 November (Dubai, UAE): David Naccache
- PriSec – 3-5 December (Sydney, Australia): David Naccache
- Botconf – 3-5 December (Paris, France): David Naccache
- ASIACRYPT – 7-11 December (Kaoshiung, Taiwan): Itai Dinur
- Indocrypt – 14-17 December (New Delhi, India): David Naccache
- INTRUST – 16-17 December (Beijing, China): David Naccache

7.1.3. Editorial Boards of Journals

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 Engineering*: David Naccache (editor)
- of *Encyclopedia of Cryptography and Security*: David Naccache (editor)
- of *Journal of Computer Security, IOS Press*: David Naccache
- of *Open Journal of Information Security and Applications, SOP*: David Naccache (editor)
- of *Cryptologia* – Taylor & Francis: David Naccache (editor)
- of *Computers & Security* – Elsevier: David Naccache
- 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

7.2. Teaching - Supervision - Juries

7.2.1. 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: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: Hoeteck Wee, Randomness in Complexity, 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

7.2.2. Supervision

- PhD: Tancrède Lepoint, Design and Implementation of Lattice-Based Cryptography, ENS, June 30th, 2014, David Pointcheval
- PhD in progress: Sylvain Ruhault, Randomness in cryptography, from 2011, David Pointcheval & Damien Vergnaud
- PhD in progress: Sonia Belaid, Leakage-resilient cryptography, from 2012, Michel Abdalla
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, from 2012, Michel Abdalla & David Pointcheval
- PhD in progress: Diana Maimut, Fully Homomorphic Encryption, from 2012, David Naccache
- PhD in progress: Thomas Prest, Lattice-based cryptography, from 2012, Vadim Lyubashevsky & David Pointcheval
- PhD in progress: Olivier Sanders, Delegation of computations, from 2012, David Pointcheval
- PhD in progress: Jérémie Clément, Lightweight cryptography, from 2013, David Naccache
- PhD in progress: Simon Cogliani, Authenticated Encryption, from 2013, David Naccache
- PhD in progress: Mario Cornejo, Security for the cloud, from 2013, Michel Abdalla
- PhD in progress: Houda Ferradi, Biometric protocols and mobile security, from 2013, David Naccache
- PhD in progress: Alain Passelègue, Security against related-key attacks, from 2013, Michel Abdalla
- PhD in progress: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, from 2013, Damien Vergnaud
- PhD in progress: Florian Bourse, Encryption Schemes for the Cloud, from 2014, Michel Abdalla & David Pointcheval
- PhD in progress: Geoffroy Couteau, Efficient secure two-party computation for the Cloud, from 2014, David Pointcheval & Hoeteck Wee
- PhD in progress: Rafael Del Pino, Lattice-Based Cryptography – Complexity and Ideal-Lattices, from 2014, Vadim Lyubashevsky
- PhD in progress: Rémi Géraud, Provable security in public-key cryptography, from 2014, David Naccache
- PhD in progress: Pierrick Meaux, Lattice-Based Cryptography – Advanced Features, from 2014, Vadim Lyubashevsky

7.2.3. Juries

- PhD Robert Künnemann. *On the Analysis of Security APIs and Stateful Protocols* – ENS Cachan – France, January 7th 2014: David Pointcheval
- HdR Emmanuel Prouff. *Analyse des Attaques par Canaux Auxiliaires et Preuves de Sécurité* – Université Pierre et Marie Curie, Paris – France, January 27th 2014: David Pointcheval
- PhD Thomas Peters. *Privacy Enhancing Cryptographic Mechanisms with Public Verifiability* – Université Catholique de Louvain – Belgium, April 2nd 2014: David Pointcheval
- PhD Alain Patey. *Techniques cryptographiques pour l'authentification et l'identification biométriques respectant la vie privée* – Telecom ParisTech – France, May 20th 2014: David Pointcheval (Chair)
- PhD Susan Thomson. *Public-Key Cryptography with Joint and Related-Key Security* – ENS – France, June 18th 2014: Michel Abdalla (Examiner)
- PhD Tancrède Lepoint. *Design and Implementation of Lattice-Based Cryptography* – ENS – France, June 30th 2014: David Naccache, David Pointcheval (Supervisor)

- HdR Damien Vergnaud. *Primitives et constructions en cryptographie asymétrique* – Ecole Normale Supérieure – France, July 1st 2014: Michel Abdalla, David Pointcheval
- PhD Slim Bettaieb. *Signature et identification pour l'anonymat, basées sur les réseaux* – Université de Limoges – France, September 26th 2014: Damien Vergnaud (Reviewer)
- PhD Adeline Langlois. *Lattice-Based Cryptography: Security Foundations and Constructions* – ENS Lyon – France, October 17 2014: Vadim Lyubashevsky (Jury member)
- HdR: Duong Hieu Phan. *Some Advances in Broadcast Encryption and Traitor Tracing* – Ecole Normale Supérieure – France, November 19th 2014: Michel Abdalla, David Pointcheval (Supervisor)
- PhD Cédric Murdica. *Sécurité Physique de la Cryptographie sur Courbes Elliptiques* – Télécom ParisTech – France, February 13th 2014: David Naccache (Supervisor)
- PhD Thomas Souvignet. *L'expertise et la lutte contre la fraude monétaire* Université Panthéon-Assas Paris 2 – France, December 18th 2014: David Naccache (Supervisor)
- PhD Jean-Michel Cioranescu. *Nouvelles contre-mesures pour la protection de circuit intégrés* – Université Panthéon-Sorbonne Paris 1 – France, December 18th 2014: David Naccache (Supervisor)
- PhD Guillaume Bouffard. *A Generic Approach for Protecting Java Card Smart Card Against Software Attacks* Université de Limoges – France, October 10th 2014: David Naccache (Reviewer)
- PhD Emmanuel Volte. *Miroirs, cubes et Feistel dissymétrique* – Université Cergy-Pontoise – France, November 28th 2014: David Pointcheval (Chair)
- PhD Rodolphe Lampe. *Preuves de sécurité en cryptographie symétrique à l'aide de la technique du coupling* – Université de Versailles Saint-Quentin en Yvelines – France, December 2nd 2014: David Pointcheval, David Naccache (Reviewer)

CRYPT Team

6. Dissemination

6.1. Promoting Scientific Activities

6.1.1. Scientific events organisation

6.1.1.1. General chair, scientific chair

- Xiaoyun Wang was General Chair of the 10th China International Conference on Information Security and Cryptology (Inscrypt 2014) in Beijing (China), from December 13 to 15, 2014.

6.1.1.2. Member of the organizing committee

- Phong Nguyen was an organizer of the LIAMA France-China 50 Workshop, in May 2014, in Paris (France).

6.1.2. Scientific events selection

6.1.2.1. Chair of conference program committee

- the 33rd IACR Eurocrypt Conference (EUROCRYPT 2014) [22]: Phong Nguyen.

6.1.2.2. Member of the conference program committee

- Eleventh Algorithmic Number Theory Symposium ANTS-XI (August 6 ? 11, 2014, Korea): Phong Nguyen.

6.1.2.3. Reviewer

The members of the team reviewed numerous papers for numerous international conferences.

6.1.3. Journal

6.1.3.1. Member of the editorial board

- 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

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

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

PhD: Phong Nguyen, Introduction to Lattice Algorithms, 3h, EPFL Winter School, Switzerland.

6.2.2. Supervision

PhD: Wei Wei, New Transference Theorems on Lattices Possessing Gaps, Tsinghua, June 2014, Xiaoyun Wang

PhD: Feng Zhang, Theory, Algorithm and Applications for Solving SVP and CVP in Lattices, CAS, Summer 2014, Yanbin Pan

6.2.3. Juries

PhD: Wei Wei, New Transference Theorems on Lattices Possessing Gaps, Tsinghua, June 2014, Xiaoyun Wang (supervisor)

PhD: Chenggang Wu, Property Testing and Related Problems, Tsinghua (Institute for Interdisciplinary Information Sciences), June 2014, Phong Nguyen (Jury member)

PhD: Feng Zhang, Theory, Algorithm and Applications for Solving SVP and CVP in Lattices, CAS, Summer 2014, Yanbin Pan (supervisor)

6.3. Popularization

Phong Nguyen gave several invited talks:

- [17] at the First NTU-VIASM Workshop on Discrete Mathematics, in Vietnam.
- at the 2014 CTIC-IIS Theory of Cryptography workshop, in China.
- at the Mathematical Workshop of the Chinese Association for Cryptologic Research, in China.

GALAAD2 Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Evelyne Hubert was invited to organize the workshop *Symbolic Analysis* at the conference Foundation of Computational Mathematics in Montevideo (December 2014).

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committee

Evelyne Hubert was a member of the program committee of the ACM conference ISSAC 2014 in Kobe (July 2014).

Bernard Mourrain was a member of the program committee of the ACM conference SNC 2014 in Shanghai (July 2014).

9.1.3. Journal

9.1.3.1. Member of the editorial board

Evelyne Hubert is an associate editor of the Journal of Symbolic Computation (since 2007).

Bernard Mourrain is an associate editor of the Journal of Symbolic Computation.

9.1.3.2. Reviewer

Laurent Busé wrote reviews for the ISSAC 2014 conference and for the following journals: Graphical Models, Linear Algebra and its Applications, Foundations of Computational Mathematics, Transactions on Visualization and Computer Graphics, Computer Aided Geometric Design, Journal of Algebra, Expert Systems with Applications, Proceedings of the London Mathematical Society, Journal of Symbolic Computation and Vietnam Journal of Mathematics. He also wrote reviews for the NSA Mathematical Sciences Grant Program.

Evelyne Hubert wrote reviews for the Journal of Symbolic computation, the Foundation of Mathematical Computing journal, the Journal of Pure and Applied Algebra, Mathematics of Computations, Plos One, Theoretical Computer Science, and for the conference proceedings of ISSAC and SNC. She was also part of the selection committee for Fulbright grants.

Bernard Mourrain wrote reviews for the followings journals: Journal of Symbolic computation, Foundation of Mathematical Computing journal, Journal of Pure and Applied Algebra, Linear Algebra and its Applications, Applicable Algebra in Engineering, Communication and Computing, Computer Aided Geometric Design, Theoretical Computer Science, Computing Surveys, SIAM Journal on Matrix Analysis and Applications, and for the conference proceedings of ISSAC and SNC, MTNS.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Mathieu Collowald, Maths (Exercices), 25h ETD, L1 SV, University of Nice-Sophia Antipolis.

Licence: Mathieu Collowald, Discrete maths (Exercices), 18h ETD, L1 I, University of Nice-Sophia Antipolis.

Licence: Mathieu Collowald, Algebra1 (Exercices), 40h ETD, L1 I, University of Nice-Sophia Antipolis.

Licence: Mathieu Collowald, Algebra2 (Exercices), 40h ETD, L1 I, University of Nice-Sophia Antipolis.

Licence: Marta Abril Bucero, Statistiques (Exercices), 20h ETD, L2 I, University of Nice-Sophia Antipolis.

Licence: Marta Abril Bucero, Analyse (Exercices), 40h ETD, L2 PC, University of Nice-Sophia Antipolis.

Master : Laurent Busé, Curves and Surfaces, 66h ETD, M1, EPU of the university of Nice-Sophia Antipolis.

Master : Laurent Busé, Elimination matrices for geometric modeling, 40h ETD, M2, math department of the university of Nice-Sophia Antipolis.

Master : Laurent Busé, Elimination matrices and applications, 18h ETD, M2, math department of the university of Buenos Aires, Argentina.

Master: Bernard Mourrain, Algorithmique des Courbes et Surfaces, M2 ACSYON, Limoges. 6h.

Doctoral courses: Bernard Mourrain, Effective Algebraic Geometry and Applications. Central European University, Budapest. 12h.

Doctoral courses: Bernard Mourrain, Sparse modelling, tensor decomposition, algorithms and applications. Summer School on An Interdisciplinary Approach to Tensor Decomposition, Trento Italy. 6h.

9.2.2. Supervision

PhD : Marta Abril Bucero, Moment matrices, real algebraic geometry and polynomial optimization, supervised by Bernard Mourrain, university of Nice-Sophia Antipolis, defended December 12th.

PhD in progress: Elisa Berrini, Parametric modeling for ship hull deformation and optimization. CIFRE with MyCFD. Started in January 2014. Supervised by Bernard Mourrain.

PhD in progress : Mathieu Collowald, Integral representation of shapes for feature conservation or extraction, started in 2011, supervised by Evelyne Hubert.

Laurent Busé supervised :

- The master thesis of Danny Schmitt, “Représentations matricielles des courbes et hypersurfaces rationnelles”, university of Nice-Sophia Antipolis,
- Anna Karasoulou, 3 months during its PhD thesis at the university of Athens under the supervision of I. Emiris, “Discriminant of a symmetric homogeneous polynomial”.
- Jingjing Shen, co-supervised with P. Alliez, 3 months during its PhD thesis at Cambridge under N. Dodgson, “Isotropic triangle meshing of nurbs models”.

9.2.3. Juries

Laurent Busé was a reviewer and a member of the PhD committee of Yacine Bouzidi, “Résolution de systèmes bivariés et topologie de courbes planes” under Sylvain Lazard and Marc Pouget, defended March 18th 2014 at the university of Lorraine (Inria Nancy), France.

Laurent Busé was a member of the PhD committee of Claire Tête, “Profondeur, dimension et résolutions en algèbre commutative: quelques aspects effectifs” under Lionel Ducos, defended October 21st 2014 at the university of Poitiers, France.

Laurent Busé was a reviewer and a member of the PhD committee of Kamran Lamei, “Fonction de Hilbert non standard et nombres de Betti gradués des puissances d’idéaux” under Marc Chardin, defended December 18th 2014 at the university Paris 6, France.

Bernard Mourrain was a reviewer and member of the PhD committee of Jeremy Veysset, “Anisotropic mesh adaptation and stabilized finite elements methods for solving conjugate heat transfers and turbulent flows” supervised by E. Hachem and Th. Coupez, September 29th, Mines ParisTech.

Bernard Mourrain was a reviewer and member of the PhD committee of Heidi Dahl, “Improved blends between primitive surface” under the supervision of Rimvydas Krasauskas, October 23th, University of Oslo.

Bernard Mourrain was a reviewer and member of the PhD committee of Jules Svartz, “Résolution des Systèmes Polynomiaux de Dimension Zéro” under the supervision of J.C. Faugère, October 30th, University Pierre et Marie Curie, Paris.

Bernard Mourrain was supervisor and member of the PhD committee of the PhD thesis of Marta Abril-Bucero, “Moment matrices, real algebraic geometry and polynomial optimization”, December 12th, University of Nice-Sophia Antipolis.

GEOMETRICA Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

Monique Teillaud co-organized the “Workshop on Geometric Structures with Symmetry and Periodicity”, part of the Computational Geometry Week 2014, with Ileana Streinu (Smith College, Northampton, MA), in Kyoto University, Japan, June 8-9. http://www-sop.inria.fr/geometrica/events/wocg14-symmetry_and_periodicity/

Jean-Daniel Boissonnat organized the first GUDHI workshop in Sophia Antipolis, October 27-29. <https://project.inria.fr/gudhi/first-gudhi-workshop/>

9.1.2. Scientific events selection

9.1.2.1. responsible of the conference program committee

Olivier Devillers was program co-chair of 2014 Symposium on Computational Geometry.

9.1.2.2. member of the conference program committee

Monique Teillaud, European Symposium on Algorithms, ESA, <http://algo2014.ii.uni.wroc.pl/esa/>

9.1.2.3. member of the steering committee

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

Monique Teillaud is a member of the Steering Committee of the European Symposium on Algorithms (ESA).

9.1.3. Journal

9.1.3.1. member of the editorial board

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

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.

9.1.4. Inria committees

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

Monique Teillaud was a member of the Inria Evaluation Committee until August.

She was a member of the national Inria DR2 interview committee and the local CR2 interview committees in Nancy and Lille.

She was also a member of the Advanced and Starting “Research Positions” interview committees.

Monique Teillaud was a member of the local Committee for Technologic Development until her move to Nancy.

She was also a member of the local committee for transversal masters.

9.1.5. National committees

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

Frédéric Chazal was a member of the Comités d'évaluation scientifique "Mathématiques et Informatique Théorique" of the ANR.

9.1.6. Web site

M. Teillaud is maintaining the Computational Geometry Web Pages <http://www.computational-geometry.org/>, hosted by Inria Sophia Antipolis until November. 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.

9.1.7. 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

Master : J.D. Boissonnat, C. Maria, M. Yvinec, *Algorithmic Geometry of Triangulations*, 24h, International Master Sophia Antipolis.

Master : S. Oudot, *Computational Geometry: from Theory to Applications*, 18h, École polytechnique.

Master : S. Oudot, *Geometric Methods for Data Analysis*, 12h, École Centrale Paris.

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

M. Teillaud, *Génération de maillages dans la bibliothèque CGAL*, in the framework of a training course for young researchers (PhD students and master students on environmental sciences) on modelling, organized by ECCOREV, 3h, Aix-en-Provence.

9.2.2. Supervision

HDR: Steve Oudot, Persistence Theory: From Quiver Representations to Data Analysis [14], Université Paris-Sud, November 26th 2014.

PhD : Clément Maria, Algorithms and Data Structures in Computational Topology [13], Université de Nice Sophia Antipolis, October 28, 2014, Jean-Daniel Boissonnat.

PhD: Ross Hemsley, Probabilistic methods for the analysis of algorithms on random tessellations [12], Université de Nice Sophia Antipolis, December 16, 2014, Olivier Devillers.

PhD: Mickaël Buchet, Topological and geometric inference from measures [11], Université Paris XI, December 2014, Frédéric Chazal and Steve Oudot.

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

PhD in progress: Mathieu Carrière, Topological signatures for geometric shapes, started in November 2014, Steve Oudot.

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

PhD in progress: Eddie Amaari, A statistical approach of topological Data Analysis, started on Sept. 2014, Frédéric Chazal (co-advised with Pascal Massart).

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.

PhD in progress : Alba Chiri de Vitis, Computational Geometry in High Dimensions, started February 2014. Jean-Daniel Boissonnat and David Cohen-Steiner.

9.2.3. Juries

Monique Teillaud was a member of the HDR defense committee of Francis Lazarus (univ. Grenoble).

Monique Teillaud was a member of the PhD defense committee of Yacine Bouzidi (Univ. de Lorraine).

Monique Teillaud was a member of the PhD defense committee (member of the three-member advisory committee) of Vissarion Fisikopoulos (Univ. Athens, Grece).

Monique Teillaud was a member of the PhD defense committee of Arnaud de Mesmay (École Normale Supérieure).

Jean-Daniel Boissonnat was a member of the HDR defense committees of Q. Mérigot and S. Oudot.

Frédéric Chazal was a member (reviewer) of the PhD defense of Arnaud de Mesmay (Ecole Normale Supérieure de Paris).

Frédéric Chazal was a member of the PhD defense of Clément Levrard (Université Paris-Sud).

Steve Oudot was a member of the PhD defense of Clément Maria (Université Nice Sophia Antipolis).

Marc Glisse was a member of the PhD defense committee of Octavio Razafindramanana, Université François Rabelais de Tours.

9.2.4. Internships

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

François Godi, Computing the bottleneck distance for persistence diagrams (Jean-Daniel Boissonnat)

Venkata Yamajala, Equating the witness and the Delaunay complexes (Jean-Daniel Boissonnat)

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

Eddie Aamari, topological Data Analysis (F. Chazal)

Mathieu Carrière, local topological signatures for shapes (S. Oudot)

9.3. Popularization

Thomas Bonis and Mathieu Carrière presented the *Photomaton 3d* at the *Fête de la Science* in October 2014. This animation consists in scanning a volunteering person in 3d using a Kinect and dedicated software, then illustrating the concepts of 3d shape comparison, retrieval and matching.

GRACE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

- D. Augot is member of the committee of the **CCA** seminar on coding and cryptology. This seminar regularly attracts around 30 participants.
- J. Nielsen, with L. de Feo, organized a Digiteo event **CLIC** related to J. Nielsen's Ditigeo funding **IDEALCODES**. This non-recurrent event attracted 30 participants.

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

- D. Augot was a member of the WAIFI 2014 programm committee (International Workshop on the Arithmetic of Finite Fields, Gebze, Turkey)

9.1.3. Reviewer

- D. Augot was a reviewer for ITW (Information Theory Workshop) 2015.
- B. Smith was a reviewer for Eurocrypt 2014, CRYPTO 2014, PKC (Public Key Cryptography) 2014, and ANTS (Algorithmic Number Theory Symposium) 2014.

9.1.4. Journal

9.1.4.1. member of the editorial board

- D. Augot is member of the editorial board of the *RAIRO - Theoretical Informatics and Applications*, a Cambridge journal published by EDP Sciences.
- D. Augot is member of the editorial board of the *International Journal of Information and Coding Theory*, InderScience publishers.

9.1.4.2. reviewer

- D. Augot was reviewer for
 - *Designs, Codes and Cryptography*;
 - *Discrete Mathematics*.
 - *IEEE Transactions in Information Theory*;
- A. Couvreur was reviewer for
 - *Design, Codes and Cryptography*;
 - *Finite Fields and Their Applications*;
 - *IEEE Transactions on Communication*;
 - *Journal of Symbolic Computation*.
- B. Smith was a reviewer for
 - *Designs, Codes and Cryptography*
 - *Mathematics of Computation*
 - *ETRI Journal*

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master

- D. Augot, Error-correcting codes and applications to cryptography, 6h00, level M2, MPRI, France.
- A. Couvreur, Error-correcting codes and applications to cryptography, 12h, level M2, MPRI, France.
- A. Couvreur is *Chargé d'enseignement* at the École Polytechnique for the academic year 2014-2015.
- A. Couvreur gave a one-week crash course in cryptology at the university of Masuku (Franceville, Gabon). Level M1.
- B. Smith, Algorithmes arithmétiques pour la cryptologie, 13.5h (equiv TD), level M2, MPRI, France.
- F. Morain, Algorithmes arithmétiques pour la cryptologie, 9h (equiv TD), M2, level M2, MPRI, France.
- B. Smith, Cryptologie, 18h (equiv TD), M1, École polytechnique, France
- F. Morain, 9 lectures of 1.5h, 3rd year (M1) course “cryptology” at École polytechnique.
- F. Levy-dit-Vehel, “Cours de Cryptographie”, 30h. (equiv TD), 3rd year (M1), ENSTA ParisTech, France.

Licence

- F. Morain 10 lectures of 1.5h, 1st year course “Introduction à l’informatique” (INF311) at École polytechnique (L3). Responsibility of this module (350 students).
- B. Smith Introduction à l’informatique, 40h (equiv TD), L3, École polytechnique, France course “Introduction à l’informatique” (INF311) at École polytechnique (L3).
- A. Couvreur Introduction à l’informatique, 40h (equiv TD), L3, École polytechnique, France course “Introduction à l’informatique” (INF311) at École polytechnique (L3).
- A. Couvreur Les bases de la programmation et de l’algorithmique, 32h (equiv TD), M1, École polytechnique, France course (INF411) at École polytechnique (M1).
- F. Levy-dit-Vehel, “Mathématiques discrètes pour la protection de l’information”, 24h. (equiv TD), 2nd year (L3), ENSTA ParisTech, France.

E-learning

- I. Márquez-Corbella, with D. Augot’s help, is currently preparing a MOOC on *code-based cryptology*. This MOOC is intended for an audience of M2 or PhD students who are interested in this sub-branch of cryptology. This can bring in students from coding theory, cryptology, or even physicists interested in post-quantum cryptography. N. Sendrier and M. Finiasz will complement and bring scientific authority to these lectures, by addressing more advanced topics. This bilingual MOOC (Spanish and English) is planned to be open in March, with a five week duration. It is supported by the Inria MOOC Lab, and will be hosted on the platform FUN.

9.2.2. Supervision

- D. Augot, advised two students, Gaspard Ferey and Sylvain Colin, for a “Projet personnel en laboratoire”, whose object of study was attacks on code-based cryptosystems and their relation to the Chor-Rivest cryptosystem. 12h, level M1, Polytechnique, France.
- A. Couvreur advised one student, Alexander Schaub, for a “Projet personnel en laboratoire” on an oblivious transfer protocol using a noisy channel. 12h, level M1, Polytechnique, France.

- A. Couvreur advised the Masters thesis of Elise Barelli (Master Cryptis, University of Limoges). 6 month internship, level M2.
- B. Smith supervised Charlotte Scribot's Masters thesis (Master P7). 6 month internship, level M2.
- B. Smith co-supervised the third year of Cécile Gonçalves' PhD project.
- F. Levy-dit-Vehel supervised Julien Lavauzelle's end of ENSTA studies internship (level M2), 5 months.

9.2.3. Juries

- D. Augot was a member of Maurice Denise's PhD committee, for her defense "Codes correcteurs quantiques pouvant se décoder itérativement", June 26th.
- D. Augot was a member of Nicolás Bordenabe's PhD committee, for his defense "Measuring Privacy with Distinguishability Metrics: Definitions, Mechanisms and Application to Location Privacy", September 12th.
- D. Augot was a reviewer of Clément Pernet's HDR thesis "High Performance and Reliable Algebraic Computing", and member of his defense committee, November 21st.
- A. Couvreur is a member of the jury of the *agrégation de mathématiques*.
- B. Smith was a member of Ivan Boyer's PhD jury, for his defense "Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe", January 24th.
- B. Smith was a member of Jean-Christophe Zapalowicz's PhD jury for his defense "Sécurité des générateurs pseudo-aléatoires et des implémentations de schémas de signature à clé publique", November 21st.

9.3. Invitations to seminars and conferences

- D. Augot made a presentation, "Décodage des codes de Reed-Solomon et logarithme discret dans les corps finis", at the Cryptography Seminar of Université de Rennes I, March 21st
- D. Augot made a presentation for the Secret project-team at Inria Rocquencourt "Bitcoin hors-sol", November 13th.
- A. Couvreur was an invited speaker at *Journées Codage et Cryptographie*, Grenoble in march 2014.
- A. Couvreur has been invited to give a talk at regular seminars in Rennes, Caen, University Paris 6, University Paris 8 and Bordeaux.
- B. Smith was an invited speaker at *YACC 2014*, Porquerolles, June 2014.
- B. Smith was an invited speaker in the *Computational Number Theory* workshop at *FOCM 2014*, Montevideo, Uruguay, December 2014.
- B. Smith was an invited speaker at the inaugural *MCrypt Workshop*, Les Deux Alpes, August 2014.
- B. Smith was an invited speaker at *DLP2014* (Theoretical and Practical Aspects of the Discrete Logarithm Problem), Ascona, Switzerland, May 2014.
- B. Smith gave a talk in the regular *PolSys* seminar at UPMC, March 2014.

9.4. Popularization

- D. Augot made a presentation "Quand $1 \oplus 1$ égal 0" at Lycée Albert Einstein, Sainte-Geneviève-des-Bois, May 19th.
- J. Piantant was one of the presenters for Inria's stand at « **Bouge la Science** » at Supélec.
- A. Couvreur gave a conference "Les mathématiques pour protéger l'information" for the pupils of Collège Moreau in Monthléry (91).

9.5. Institutional commitment

- A. Couvreur is an elected member of Saclay's *comité de centre*.
- A. Couvreur was a member of the commission for the recruitment of post-doc researchers in 2014 at LIX in the programm Qualcomm-Carnot.
- A. Couvreur is the *jeune chercheur référent* for the *commission de suivi doctoral* of Inria Saclay.
- D. Augot was a member of RTRA Digiteo program committee.
- D. Augot is a member of LIX's *conseil de direction*.
- D. Augot is a member of the *conseil de l'école doctorale en informatique de Paris-Sud*
- D. Augot is the vice-head of Inria's *comité de suivi doctoral*
- D. Augot is a member of LIX's *conseil de laboratoire*
- D. Augot and B. Smith were reviewers for ANRT CIFRE fundings.
- F. Morain, J. Pielant and B. Smith are elected members of the *Conseil de Laboratoire* of the LIX.
- F. Morain is vice-head of the Département d'informatique of Ecole Polytechnique.
- F. Morain represents École polytechnique in the committee in charge of *Mention HPC* in the *Master de l'université Paris Saclay*.
- B. Smith is a *Correspondant* for International Relations at Saclay.
- B. Smith is a member of the COST-GTRI.
- B. Smith is a member of the teaching committee of the Department of Computer Science of the École polytechnique.

LFANT Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific events organisation

7.1.1.1. member of the organizing committee

The team helped organising the **Colloque Jeunes Chercheurs en Théorie des Nombres**, which took place in Bordeaux on 11/06/2014–13/06/2014.

7.1.2. Scientific events selection

7.1.2.1. member of the conference program committee

Andreas Enge was a member of the programme committee for the *Elliptic Curve Cryptography* 2014 conference in Chennai, India.

Sorina Ionica was a member of the program committee for the *Latincrypt* 2014 conference.

7.1.3. Journal

7.1.3.1. member of the editorial board

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.

7.1.4. Other scientific activities

7.1.4.1. Invited talks

- D. Robert was invited to give a talk on “Pairings on abelian varieties and the Discrete Logarithm Problem” for the Discrete Logarithm Problem Conference in May 2014 at Ascona, Switzerland
- D. Robert was invited to give a talk on “Isogenies between abelian varieties” for the Effective moduli spaces and applications to cryptography conference in June 2014 at Rennes
- D. Robert was invited to give a talk on “Optimal pairings on abelian varieties” for the Elliptic Curve Cryptography conference in October 2014 at Chennai, India
- H. Ivey-Law was invited to give a talk on “Arithmetic on Jacobians of Relative Curves” for the Number Theory Meets Geometry conference in November 2014 at Kaiserslautern, Germany
- A. Enge has given an invited talk on “Abelian varieties and theta functions for cryptography” at the 4th International Cryptology and Information Security Conference at Putrajaya, Malaysia
- A. Enge has given an invited talk on “Class invariants for Abelian surfaces” at the workshop Computational Number Theory of Foundations of Computational Mathematics in Montevideo, Uruguay

7.1.4.2. Seminar

The following external speakers have given a presentation at the LFANT seminar, see

<http://lfant.math.u-bordeaux1.fr/index.php?category=seminar>

- Frédérique Oggier (NTU, Singapour): “Le codage pour le stockage distribué de données”
- Hartmut Monien (Physikalisches Institut der Universität Bonn): “Zeta values, random matrix theory and Euler-MacLaurin summation” and “Calculating rational coverings for subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ efficiently”
- Nicolas Delfosse (Montreal): “Une introduction au calcul quantique tolérant aux fautes”
- Eduardo Friedman (Universidad de Chile): “Cône de Shintani et degré topologique”
- John Boxall (Caen): “Heuristiques sur les variétés abéliennes adaptées à la cryptographie à couplage”
- Pınar Kılıçer (Leiden+IMB): “The class number one problem for genus-2 curves”
- Bertrand Maury (Paris-Sud): “Arbre bronchique infini et entiers dyadiques”
- Emmanuel Thomé (Nancy): “Un algorithme quasi-polynomial de calcul de logarithme discret en petite caractéristique”
- Oriol Serra (UPC, Barcelone): “Algebraic Removal Lemma”
- Amalia Pizarro-Madariaga (Valparaíso): “Estimations for the Artin conductor”
- Alina Dudeanu (EPFL): “Computing a Velu type formula for rational cyclic isogenies between isomorphism classes of Jacobians of genus two curves that are defined over a finite field.”
- Gaetan Bisson (University of French Polynesia): “On polarised class groups of orders in quartic CM-fields”
- Kamal Khuri Makdisi (American University of Beirut): “Moduli interpretation of Eisenstein series”
- Kamal Khuri Makdisi (American University of Beirut): “On divisor group arithmetic for typical divisors on curves”
- Chloe Martindale (University of Leiden / IMB): “An algorithm for computing Hilbert modular varieties”
- Dimitar Jetchev (EPFL): “Euler systems from special cycles on unitary Shimura varieties and arithmetic applications”
- Alain Couvreur (Inria and LIX, École Polytechnique): “Une attaque polynomiale du schéma de McEliece basé sur les codes de Goppa "sauvages".”

7.1.4.3. Research administration

K. Belabas is vice-head of the Math Institute (IMB). He also leads the computer science support service (“cellule informatique”) of IMB and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

He is an elected member of “commission de la recherche” in the academic senate of Bordeaux University.

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*.

A. Enge is the head of the COST-GTRI, the Inria body responsible for the scientific evaluation of the international partnerships of the institute.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Summer school: A. Enge, Complex multiplication of elliptic curves and Pairings on elliptic curves, 6h, Putrajaya, Malaysia

Master: K. Belabas, Computer Algebra, 90h, M2, Université de Bordeaux

Master: K. Belabas, Computational number theory, 50h, M2, Université de Bordeaux

Master: K. Belabas, Number theory, 24h, M1, Université de Bordeaux

Licence: K. Belabas, C2i, 24h, L1, Université de Bordeaux

Licence: Jean-Paul Cerri, Codes et cryptologie, 34.67h, TD niveau L1, Université de Bordeaux

Licence: Jean-Paul Cerri, Algèbre 4, 50.67h, TD niveau L3, Université de Bordeaux

Licence: Jean-Paul Cerri, Cryptographie et Arithmétique, 24h, Cours niveau L3, Université de Bordeaux

Master, Jean-Paul Cerri, Arithmétique, 36h, Cours niveau M1, Université de Bordeaux

Encadrement, Jean-Paul Cerri, Encadrement d'un projet tuteuré (L3) et d'un TER (M1), Université de Bordeaux

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

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

Licence : E. Milio, Topologie et Fonctions de plusieurs variables, 36 heures, niveau L2, université de Bordeaux site Victoire, France

Master: Sorina Ionica, Encadrement de 3 projets master (M2 CSI), Université de Bordeaux.

7.2.2. Supervision

PhD: Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, [12], supervised by K. Belabas and A. Enge, defended 07/2014

PhD: Nicolas Mascot, *Computing modular Galois representations* [11], supervised by K. Belabas and J.-M. Couveignes, defended 07/2014

PhD in progress: Enea Milio, *Isogénies entre surfaces abéliennes*, University Bordeaux, supervised by A. Enge and D. Robert

PhD in progress: Pınar Kılıçer, *Topics in complex multiplication*, Universities Bordeaux and Leiden, supervised by A. Enge and M. Streng

PhD in progress: Chloë Martindale, *Isogeny graphs*, Universities Bordeaux and Leiden, supervised by A. Enge and M. Streng

7.2.3. Juries

D. Robert was a member of the committee for the PhD defense of Christophe Tran in Rennes (December 2013).

A. Enge was a referee for the PhD of Nicole Sutherland, University of Sydney, entitled “Algorithms for Galois extensions of Global Function Fields”.

7.3. Popularization

K. Belabas gave a lecture to present Bhargava’s works (2014 Fields medal) to high school teachers during the “Journée de l’IREM d’Aquitaine” (11/2014, about 100 attendants).

A. Enge has presented “Les maths au service du secret (et de sa découverte!)” during the Math en Jeans congress held in Bordeaux in April 2014, for an audience of highschool pupils aged 12 to 17.

He has spoken on “Mathematik für (und gegen!) das Geheimnis” in an event in July at Gymnasium Leopoldinum, Detmold, Germany, to an audience comprised of pupils aged 12 to 18 and of mathematics teachers.

At the GNU Hacker’s Meeting 2014 in München, Germany, he has presented a tutorial on “GnuPG key signing”.

POLSYS Project-Team

8. Dissemination

8.1. POLSYS seminar

Our seminar hosted over twenty invited speakers in 2014.

<http://www-polsys.lip6.fr/Seminar/index.html>

8.2. Promoting Scientific Activities

8.2.1. Scientific events organisation

8.2.1.1. member of the organizing committee

Dongming Wang was involved in the organization of the following conferences

- Third International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2014) (Vienna, Austria, July 17-18, 2014).
- Software for Geometry at the 4th International Congress on Mathematical Software (ICMS 2014) (Seoul, Korea, August 5-9, 2014).

8.2.2. Scientific events selection

8.2.2.1. member of the conference program committee

Ludovic Perret was member of the program committee of the following conference:

- Eurocrypt 2014 is the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (11 - 15 May 2014 Copenhagen, Denmark)

Mohab Safey El Din was member of the program committee of the following conferences:

- 39-th Symposium on Symbolic and Algebraic Computation (ISSAC 2014) (Kobe, Japan, July 23-25, 2014)
- ACM Symbolic-Numeric Computation Conference (SNC 2014) (Shanghai, China, July 28-31, 2014)

Jean-Charles Faugère and Ludovic Perret were involved in a special Issue of the Journal Of Symbolic Computation (JSC) devoted to Mathematical and Computer Algebra Techniques in Cryptology.

Jean-Charles Faugère was member of the program committee of the following conferences:

- 39-th Symposium on Symbolic and Algebraic Computation (ISSAC 2014) (Kobe, Japan, July 23-25, 2014)
- The IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'2015)
- The thirteenth conference MEGA (University of Trento, Italy)

Elias Tsigaridas was member of the program committee of the following conferences:

- ACM Symbolic-Numeric Computation Conference (SNC 2014) (Shanghai, China, July 28-31, 2014)

Dongming Wang was member of the program committees of the following conferences

- 6th International Symposium on Symbolic Computation in Software Science (SCSS 2014) (Gammarrth, Tunisia, December 7-11, 2014),
- 16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2014) (Timisoara, Romania, September 22-25, 2014),
- 12th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2014) (Sevilla, Spain, December 11-13, 2014),
- 10th International Workshop on Automated Deduction in Geometry (ADG 2014) (Coimbra, Portugal, July 9-11, 2014).

8.2.3. Journal

8.2.3.1. member of the editorial board

Ludovic Perret is member of the editorial board of Designs, Codes and Cryptography published by Springer.

Mohab Safey El Din is member of the editorial board of Journal of Symbolic Computation (published by Academic Press/Elsevier, London).

Dongming 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).

8.2.4. Invited Talks

Jean-Charles Faugère was invited talk at:

- Workshop on Polynomials over Finite Fields - Barcelona - Centre de Recerca Matemàtica (CRM) - Spain
- Computational Nonlinear Algebra - Computational Nonlinear Algebra (ICERM) - Providence - USA
- Main lecture - Journées Nationales de Calcul Formel

Guénaél Renault was invited speaker for the following international conferences:

- Espaces de modules effectifs et application à la cryptographie (June 10-13, 2014, Rennes, France)
- 18th Workshop On Elliptic Curve Cryptography (October 8-10, 2014, Chennai, India)

Mohab Safey El Din was invited talk at:

- Workshop *Solving Polynomial Equations* as part of the *Algorithms and Complexity in Algebraic Geometry* program, Simons Institute, Berkeley, Oct. 2014.
- Special track on *Algebraic techniques in polynomial optimization*, IFORS, Barcelona, Spain, July, 2014.
- *Real Algebraic Geometry With A View Toward Systems Control and Free Positivity*, Oberwolfach, Germany, April, 2014.

8.3. Teaching - Supervision - Juries

8.3.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 54 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

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

Master : Introduction à la Sécurité, 32 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction au Calcul Scientifique, 40 heures équivalent TD, niveau L2, Université Pierre-et-Marie-Curie, France

Jean-Charles Faugère had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 12 heures équivalent TD, niveau M2, MPRI

Ludovic Perret had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 12 heures équivalent TD, niveau M2, MPRI

Master : Responsable Introduction à la sécurité, 96 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Responsable Complexité, 48 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction à l'Algorithmique, niveau L2, Université Pierre-et-Marie-Curie, France

Licence : Responsable en L2 du parcours informatique-mathématiques appliquées (PIMA), niveau L2, Université Pierre-et-Marie-Curie, France

Guénaël Renault had the following teaching activities:

Master : Co-responsable de la spécialité SFPN du master d'informatique, Université Pierre-et-Marie-Curie, France

Master : Responsable Cryptologie Avancée et Appliquée, 50 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Responsable Sécurité et Canaux Auxiliaires, 12 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Responsable Modélisation des attaques et des menaces, 25 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Master : Responsable Algèbre linéaire et applications, 25 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Responsable Introduction à la cryptologie, 40 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

Mohab Safey El Din had the following teaching activities:

Master : Résolution de systèmes polynomiaux, 30 heures équivalent TD, niveau M2, Université Pierre-et-Marie-Curie, France

Master : Modélisation et résolutions numérique et symbolique de problèmes *via* les logiciels MAPLE et MATLAB, 21 heures équivalent TD, niveau M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction à la Cryptologie, 20 heures équivalent TD, niveau L3, Université Pierre-et-Marie-Curie, France

8.3.2. Supervision

PhD : Jules Svartz, Résolution de Systèmes polynomiaux structurés de Dimension zéro, Université Pierre-et-Marie-Curie (Univ. Paris 6), 30 Oct. 2014, Jean-Charles Faugère

PhD in progress : Ivan Bannwarth, Fast algorithms for studying real algebraic sets, Sept. 2014, Mohab Safey El Din

PhD in progress : Simone Naldi, Exact algorithms for rank defects in linear matrices, Sept. 2012, Didier Henrion and Mohab Safey El Din

PhD in progress : Frédéric Urvoy de Portzamparc, Algebraic Cryptanalysis and Physical Attacks in Code-Based Cryptography, Fev. 2012, Jean-Charles Faugère and Ludovic Perret

PhD in progress : Thibaut Verron, Gröbner bases and structured polynomial systems, Sept. 2012, Jean-Charles Faugère and Mohab Safey El Din

PhD in progress : Rina Zeitoun, Coppersmith's Algorithm and Applications in Cryptology, Jan. 2011, Jean-Charles Faugère and Guénaél Renault

8.3.3. Juries

Jen-Charles Faugère

member of the HDR committee of Guillaume Chèze

member of the HDR committee of Frederic Chyzac

member of the HDR committee of Clement Pernet

member of the PhD committee of Ruixian Renaud as the president of the committee.

member of the PhD committee of Jules Svartz as a an examiner.

Mohab Safey El Din was:

member of the PhD committee of Marta Abril Bucerro as a reviewer;

member of the PhD committee of Pierre Lairez as a reviewer;

member of the PhD committee of Jules Svartz as a an examiner.

member of the PhD committee of Sébastien Tavenas as a reviewer;

8.4. Popularization

Guénaél Renault was invited speaker for the workshop *Fabriquer le Hazard du forum Science, Recherche et Société* (May 22, 2014) organized by the newspapers Le Monde et La Recherche.

SECRET Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

- A. Canteaut serves as a chair of 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>;
- J.-P. Tillich served as a scientific organizer of the International workshop on quantum LDPC codes, July 14-16, Waterloo (Canada).
- WCC 2015 to be held in Paris, April 13-17, 2015, is organized by the project-team. The organizing committee is composed of A. Canteaut, G. Leurent, M. Naya Plasencia.

9.1.1.2. member of the organizing committee

- QCrypt 2014: September 1-5, Paris (France): A. Leverrier.
- Advances in Quantum Cryptography Workshop, AQC 2015: March 23-24, 2015, Paris (France): A. Chailloux and A. Leverrier.

9.1.2. Scientific events selection

9.1.2.1. chair of the conference program committee

- WCC 2015: April 13-17, 2015, Paris (France): P. Charpin, N. Sendrier and J.P. Tillich (co-chairs).

9.1.2.2. member of the conference program committee

- 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, J.-P. 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);
- WAIFI 2014: September 26-28, 2014 (J.-P. Tillich);
- PQCrypto 2014: October 1-3 2014, Waterloo, Canada (N. Sendrier, J.-P. Tillich);
- Latincrypt 2014: September, 17-19, 2014, Florianópolis, Brazil (N. Sendrier);
- SETA 2014: November 24-28, 2014, Melbourne, Australia (P. Charpin);
- Asiacrypt 2014: December 7-11, 2014, China (M. Naya-Plasencia);
- Indocrypt 2014: December 14-17, 2014, New Delhi, India (A. Canteaut).
- FSE 2015: March 8-11, 2015, Istanbul, Turkey (A. Canteaut, G. Leurent, M. Naya-Plasencia);
- CT-RSA 2015: April 20-24, 2015, San Francisco, USA (M. Naya-Plasencia);
- Eurocrypt 2015: April 26-30, 2015, Sofia, Bulgaria (A. Canteaut);
- Finite Fields and their applications $F_{q^{12}}$, Saratoga, USA, July 13-17, 2015 (A. Canteaut);

- SAC 2015: August 12-14, 2015, Sackville, Canada (M. Naya-Plasencia);
- Crypto 2015: August 16-20, 2015, Santa Barbara, USA (A. Canteaut);
- National workshop on Coding and Cryptography (Journées C2), March 24-28, 2014, Les Sept Laux, France, (M. Naya-Plasencia, J.-P. Tillich).

9.1.3. Journal

9.1.3.1. member of the editorial board

- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Their Applications* associate editors: A. Canteaut, P. Charpin.
- *Annals of telecommunications*, associate editor : J.-P. Tillich.

9.1.4. Other responsibilities in the national community

- N. Sendrier is a vice-chair of the “Commission d’Evaluation” at Inria;
- A. Canteaut is a member of the “Comité de pilotage” of the Fondation Sciences Mathématiques de Paris;
- N. Sendrier served on the selection committee for “Directeurs de recherche (DR2)” at Inria;
- A. Canteaut served on the selection committee for “chargés de recherche” at the Paris-Rocquencourt Inria research center;
- N. Sendrier served on the selection committee for “chargés de recherche” at the Sophia Antipolis - Méditerranée Inria research center;
- A. Canteaut served on the selection committee for promotion to the position of associate professor at DTU (Denmark);
- A. Canteaut served on the selection committee for promotion to the position of associate professor at ISI Kolkata (India);
- J.-P. Tillich is in charge of “Formation par la recherche” for the Paris-Rocquencourt Inria center.
- A. Chailloux served on the jury for the 2014 Gilles Kahn thesis prize, November 2014, Paris.

9.1.5. Invited talks

- A. Canteaut, *Chiffrements à bas coût : comment chiffrer et déchiffrer avec des opérations similaires*, Journées Nationales du GDR Informatique Mathématique, Paris, France, January 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Quantum Information Processing - QIP 2014, Barcelona, Spain, February 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Asian Quantum Information Science Conference - AQIS 2014, Tokyo, Japan, August 2014.
- M. Naya Plasencia, *On Lightweight Block Ciphers and Their Security*, Indocrypt 2014, New Delhi, India, December 2014.
- N. Sendrier, *QC-MDPC-McEliece: A public-key code-based encryption scheme based on quasi-cyclic moderate density parity check codes*, Workshop “Post-Quantum Cryptography: Recent Results and Trends”, Fukuoka, Japan, November 3-4, 2014.
- N. Sendrier, *Best known attacks on code-based cryptosystems: state of the art and perspectives*, DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, Piscataway, NJ, USA, January 12-16, 2015.
- J.P. Tillich, *Recent attacks on McEliece schemes based on Goppa codes*, Yet Another Conference on Cryptography - YACC 2014, Porquerolles Island, France, June 2014;
- J.P. Tillich, *Turning error-reducing quantum turbo codes into error-correcting codes*, Third International Conference on Quantum Error Correction - QEC 14, Zurich, Switzerland, December 2014.

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

- G. Leurent, *New Generic Attacks on Hash-based MACs*, Dagstuhl Seminar 14021 - Symmetric Cryptography, Dagstuhl, Germany, January 2014.
- A. Leverrier, *A combinatorial approach to contextuality*, Meeting on Reliability, Security and Quality Assurance, Bordeaux, France, September 2014.
- A. Chailloux, *Strong connections between quantum encodings, non-locality and quantum cryptography*, Dimension Witness workshop - DIMWIT 2014, Sopot, Poland, June 2014.
- A. Chailloux, *Parallel repetition of entangled games via the superposed information cost*, Workshop on quantum games, Berkeley, U.S.A., February 2014.
- A. Chailloux, *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, PCQC inaugural meeting, Paris, France, August 2014.
- A. Chailloux, *Parallel Repetition of Free Entangled Games: Simplification and Improvements*, Theory Seminar of UAB, Barcelona, Spain, November 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: A. Canteaut, *Stream ciphers*, 6 hours, M1, Telecom ParisTech, France;

Master: A. Canteaut, *Introduction to symmetric cryptography*, 7 hours, M1, Telecom ParisTech, France;

Master: A. Canteaut, *Error-correcting codes and applications to cryptography*, 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 hours, M2, Ecole Polytechnique, France;

The members of the project-team also gave advanced lectures to several summer schools for PhD students:

- *Design and security of cryptographic algorithms and devices for real-world applications*, Sibenik, Croatia, June 1-6, 2014: A. Canteaut and M. Naya-Plasencia.
- *Post-Quantum Cryptography Summer School*, Waterloo, Ontario, Canada, September 29-30, 2014: N. Sendrier.

9.2.2. Supervision

PhD: Marion Bellard, *Influence of the mapping in the reverse-engineering of a communication systems*, University Pierre-et-Marie Curie, January 30, 2014, supervisor: N. Sendrier

PhD: Grégory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, University Pierre-et-Marie Curie, September 18, 2014, supervisor: N. Sendrier

PhD: Denise Maurice, *Quantum error-correcting codes with an efficient decoding algorithm*, University Pierre-et-Marie Curie, June 26, 2014, supervisor: J.-P. Tillich

PhD: Valentin Suder, *Differential properties of permutations and applications in symmetric cryptography*, University Pierre-et-Marie Curie, November 5, 2014, supervisor: P. Charpin

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

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

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

PhD in progress: Julia Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, since February 2014, CIFRE convention with Thales, supervisor: N. Sendrier

PhD in progress: Kaushik Chakraborty, *Position-based Quantum Cryptography*, since October 2014, supervisors: A. Leverrier, J.P. Tillich

PhD in progress: Adrien Hauteville, *Rank-metric-based Cryptosystems*, since October 2014, supervisors: P. Gaborit (Univ. Limoges) and J.-P. Tillich

9.2.3. Juries

- Marion Bellard, *Influence of the mapping in the reverse-engineering of a communication system*, University Pierre-et-Marie Curie, January 30, 2014, committee: N. Sendrier (supervisor) and J.-P. Tillich;
- Nathan Walk, *Continuous Variable Quantum Communication*, The University of Queensland, Australia, March 2014, A. Leverrier (reviewer).
- Florian Caullery, *Polynomials over finite fields for cryptography*, Université Aix-Marseille, May 28, 2014, A. Canteaut (chair);
- Denise Maurice, *Quantum error-correcting codes with an efficient decoding algorithm*, University Pierre-et-Marie Curie, June 26, 2014, committee: J.-P. Tillich (supervisor);
- Deng Tang, *Boolean functions for stream and block-ciphers*, Université Paris 8, July 1, 2014, A. Canteaut (chair);
- Anna Pappa, *Quantum cryptographic primitives in realistic scenarios*, Télécom ParisTech, July 10, committee: J.-P. Tillich;
- Gregory Landais, *Implementations of code-based cryptosystems and of their cryptanalyses*, University Pierre-et-Marie Curie, September 18, 2014, committee: N. Sendrier (supervisor) and J.-P. Tillich;
- Valentin Suder, *Differential properties of permutations and applications in symmetric cryptography*, Université Pierre et Marie Curie, November 5, 2014, P. Charpin (supervisor), A. Canteaut;
- François Arnault, *Contributions in discrete mathematics and cryptographic applications* (Habilitation), University of Limoges, November 12, 2014, committee: J.-P. Tillich (reviewer);
- Marion Candau, *Non Abelian convolutional codes*, University de Bretagne Occidentale, December 9, 2014, committee: J.-P. Tillich (reviewer);
- Gaétan Murat, *Weakly structured error correcting codes for the rank metric with applications to cryptography*, University of Limoges, December 9, 2014, committee: J.P. Tillich (reviewer).
- S. Raizada, *Some Results On Analysis And Implementation Of HC-128 Stream Cipher*, ISI Kolkata (India), January 2015, A. Canteaut (reviewer).

9.3. Popularization

- Anne Canteaut has been invited to give the annual Computer Science Talk for the new students at Ecole Polytechnique, Palaiseau, June 2014 [79].

SPECFUN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

- A. Bostan has served in the organizing committee of the JNCF 2014, the annual meeting of the French computer algebra community.

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

- A. Bostan has served in the program committee of the SYNASC 2014 international conference.
- A. Bostan is part of the Scientific advisory board of the MEGA conference series.
- A. Mahboubi has served in the program committee of the ITP 2014 and CICM/Calculemus 2014 international conferences.

9.1.2.2. reviewer

- A. Bostan has served as reviewer for the ISSAC 2014 and SYNASC 2014 conferences.
- F. Chyzak has served as reviewer for the conference Calculemus 2014.
- A. Mahboubi has served as reviewer for the NFM 15 and CPP 15 international conference, and for the JFLA 2015 national conference.
- C. Tankink has served as reviewer for the ITP 2014 international conference.

9.1.3. Journal

9.1.3.1. reviewer

- A. Bostan has served as reviewer for the Journal of Symbolic Computation and for the American Mathematical Monthly.
- F. Chyzak has served as reviewer for the Journal of Algebra.
- A. Mahboubi has served as reviewer for the Journal of Automated Reasoning.

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*, 6h, M2, MPRI, France
- Doctorat : A. Mahboubi, Lecturer at the *Summer School Méthodes Algorithmiques et Applications en Géométrie Algébrique Réelle et Théorie des Nombres*, 4.5h, a CIMPA School at AIMS (M'Bour, Sénégal)
- Doctorat : A. Mahboubi, Lecturer, 12h at the *NII Shonan School on Coq*, at Shonan (Japan)
- Research School : A. Mahboubi, Lecturer, 6h, at the *Introductory school to the IHP special semester on semantics of formal proofs and certified mathematics*, CIRM (Marseille, France)

9.2.2. Supervision

- HdR: F. Chyzak, *The ABC of Creative Telescoping: Algorithms, Bounds, Complexity*, University Paris-Sud 11, April 14, 2014 [1]
- PhD: P. Lairez, *Périodes d'intégrales rationnelles : algorithmes et applications*, École Polytechnique, November 12, 2014, supervised by A. Bostan and B. Salvy [2]
- PhD in progress: A. Barillec, *Asymptotique automatique certifiée des fonctions spéciales*, École Polytechnique, started in September 2013, supervised by F. Chyzak and A. Mahboubi
- PhD in progress: L. Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, École Polytechnique, started in September 2013, supervised by A. Bostan and B. Salvy
- PhD in progress: Th. Sibut-Pinote, *Calcul numérique et démonstrations mathématiques : de la rigueur à la preuve formelle*, started in September 2014, supervised by A. Mahboubi
- Master : A. Mahboubi has supervised the Master 2 internship of Thomas Sibut-Pinote (ÉNS Lyon).

9.2.3. Juries

- A. Bostan has served as a jury member of the French *Agrégation de Mathématiques – épreuve de modélisation, option C*.

9.3. Keynote talks

- A. Mahboubi has given an invited lecture at the joint CSL-LICS conference, part of the Vienna Summer of Logic 2014.
- A. Mahboubi has given an invited lecture at the “Leçons de Mathématiques et d’Informatique d’Aujourd’hui” colloquium in Bordeaux.

9.4. Popularization

- A. Mahboubi has written an article [16] for the popular science website “Images de Mathématiques”, in the context of a partnership of this website with the Bourbaki seminar.
- A. Mahboubi has given a talk at the popular science event “Nuit des Sciences, Ébullitions” <http://www.nuit-sciences.ens.fr/> at École Normale Supérieure, on June 6th 2014.
- A. Mahboubi has been interviewed by Ph. Pajot in the magazine *La Recherche*, November 2014.
- A. Mahboubi has given a “Science Break” talk, at Supélec, on December 10th 2014, an event organized by La Diagonale Paris-Saclay, part of la Fondation de Coopération Scientifique Campus-Paris-Saclay.

VEGAS Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific events organisation

7.1.1.1. Organizing committee membership

Sylvain Lazard organized with S. Whitesides (Victoria University) the 13th Inria - McGill - Victoria Workshop on Computational Geometry ⁰ at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

Marc Pouget and Guillaume Moroz organized the first ANR-SingCAST meeting on subdivision methods for singular systems in Nantes in December. ⁰

Guillaume Moroz co-organizes the *Journées Nationales de Calcul Formel 2015 (JNCF)*.

7.1.2. Scientific events selection

7.1.2.1. Conference program committee membership

Monique Teillaud is a member of the program committee of the 2015 *Symposium on Computational Geometry SoCG'15*.

7.1.2.2. Reviewing activities

All members of the team are regular reviewers for the conferences of our field, namely the *Symposium on Computational Geometry* (SoCG) and the *International Symposium on Symbolic and Algebraic Computation* (ISSAC) and also SODA, CCCG, EuroCG.

7.1.3. Journal

7.1.3.1. Editorial board membership

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*.

Marc Pouget and Monique Teillaud are members of the **CGAL** editorial board.

7.1.3.2. Reviewing activities

All members of the team are regular reviewers for the journals of our field, namely *Discrete and Computational Geometry* (DCG), *Computational Geometry. Theory and Applications* (CGTA), *Journal of Computational Geometry* (JoCG), *International Journal on Computational Geometry and Applications* (IJCGA), *Journal on Symbolic Computations* (JSC), *SIAM Journal on Computing* (SICOMP), *Mathematics in Computer Science* (MCS), etc.

⁰Workshop on Computational Geometry

⁰SingCAST

7.1.4. Steering Committees

Monique Teillaud is a member of the Steering Committee of the European Symposium on Algorithms (ESA).

7.1.5. National committees

Monique Teillaud has been a member of the Scientific Board of the Société Informatique de France (SIF) since November.

Laurent Dupont is a member of “Commission Pédagogique Nationale” (CPN) Information-Communication / Métiers du Multimédia et de l’Internet.

7.1.6. Web site

M. Teillaud is maintaining the Computational Geometry Web Pages <http://www.computational-geometry.org/>, hosted by Inria Nancy - Grand Est since December. 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.

G. Moroz is maintaining the ANR Presage website <http://webloria.loria.fr/~goaoc/ANR-Presage>

M. Pouget is maintaining the ANR SingCAST website <https://project.inria.fr/singcast/>

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Master : O. Devillers, *Synthèse, image et géométrie*, 12h (academic year 2014-15), IPAC-R, Université de Lorraine. <http://www.loria.fr/~odevil/master/>

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

Master: Guillaume Moroz, *Introduction à la résolution réelle de systèmes bivariés et topologie de courbes*, 20h (April 2014), Université de Ziguinchor, Sénégal.

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*, 70h, L1, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Programmation Objet et Évènementielle*, 50h, L2, Université de Lorraine (IUT Charlemagne).

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

Licence: Laurent Dupont, *Algorithmique*, 30h, L1, Université de Lorraine (IUT Charlemagne)

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

Licence: Yacine Bouzidi, *Programmation orientée objet*, 46h, L2, Université de Lorraine.

Master: Yacine Bouzidi, *Java avancé*, 20h, M1, Université de Lorraine.

7.2.2. Supervision

PhD in progress : Rémy Thomasse, Smoothed complexity of geometric structures and algorithms, started December 1st 2012, Olivier Devillers. (The student is hosted in EPI GEOMETRICA but supervised by O. Devillers).

PhD in progress : Ranjan Jha, Étude de l’espace de travail des mécanismes à boucles fermées, started in Oct. 2013, supervised by Damien Chablat, Fabrice Rouillier and Guillaume Moroz.

PhD in progress : Sény Diatta, Complexité du calcul de la topologie d'une courbe dans l'espace et d'une surface, started in Nov. 2014, supervised by Daouda Niang Diatta, Marie-Françoise Roy and Guillaume Moroz.

PhD: Yacine Bouzidi, Solving bivariate algebraic systems and topology of plane curves, defended in March 2014, supervised by Sylvain Lazard and Marc Pouget.

Postdoc: Rémy Imbach, Topology and geometry of singular surfaces with numerical algorithms, supervised by Guillaume Moroz and Marc Pouget.

Postdoc: Laurent Veysseire, Probabilistic analysis of geometric structures, supervised by Olivier Devillers.

7.2.3. *Juries*

O. Devillers was a member (advisor) of the PhD defense committee of Ross Hemsley (Univ. Nice - Sophia Antipolis).

M. Pouget and S. Lazard were member (advisors) of the PhD defense committee of Yacine Bouzidi (Univ. Lorraine).

G. Moroz was a member (external examiner) of the PhD defense committee of Esmail Mehrabi (Univ. of Western Ontario)

7.3. Popularization

Guillaume Moroz is a member of the organizing committee of the *Olympiades académiques de mathématiques*.

ALF Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

- Isabelle Puaut is a member of the Executive committee of IEEE Technical Committee on Real-Time Systems
- Isabelle Puaut is member of the Steering committees of ECRTS and WCET conferences.
- Isabelle Puaut is the chair of the RTNS steering committee.
- Isabelle Puaut and Damien Hardy are organizing the Ecole d'été Temps Réel in Rennes in August 2015.
- Sylvain Collange is a member of the organization committee of Rencontres Arithmétiques de l'Informatique Mathématique (RAIM) 2015 in Rennes.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committee

- Isabelle Puaut was a member of RTSS 2014, RTAS 2014, RTCSA 2014 and SIES 2014 program committees. She is a member of the RTAS 2015 and WCET 2015 program committees.
- Damien Hardy was a member of RTNS 2014 and WCET 2014 program committees. He is a member of the WCET 2015 program committee.
- André Seznec was a member of the MICRO 2014 top picks committee, a member of SAMOS 2014 program committee and HPCA 2015 committee.
- Erven Rohou was a member of the program committee of DITAM-PARMA 2015
- Pierre Michaud was a member of the program committees of the HPCC 2014 conference and the OMHI 2014 and CBP4 workshops.
- Sylvain Collange was a member of the program committee of the "Conférence en Parallélisme, Architecture et Système"(ComPas) 2014, Neuchâtel, Suisse.

9.1.3. Journal

9.1.3.1. Member of the editorial board

- André Seznec is a member of the editorial board of the IEEE Micro.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: A. Seznec, P. Michaud, A. Perais, Architecture avancée, 36 hours, M2, Ecole Supérieure d'Ingénieurs de Rennes, 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: D. Hardy, A. Perais, 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
 Master: S. Collange, Programmation parallèle, 22 hours, M1, Université de Rennes I, France
 Master/PhD: S. Collange, GPU programming, 30 hours, MSc/PhD programs, Universidade Federal de Minas Gerais, Brasil

9.2.2. Supervision

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

9.2.3. Dissemination

- Erven Rohou and Damien Hardy taught labs on "Compilation, Optimization, Debug methods" at "Ecole Jeune Chercheurs en programmation" in Rennes, June 2014
- Nabil Hallou presented "Dynamic re-vectorization of binary code", at Huitièmes rencontres de la communauté française de compilation, Jul 2014.
- Emmanuel Riou presented "Padrone: a dynamic binary modification tool" at the Intel Compiler, ARchitecture and Tools conference, at Haifa, Israel, Dec 2014
- Damien Hardy presented "Worst Case Execution Time Estimation and Permanent Faults" in the workshop on Challenges in Mixed Criticality and Real-time and Reliability in Networked Complex Embedded Systems at the Hipeac Computer System Week, May 2014.
- André Seznec and Arthur Perais presented their work on Value Prediction at a seminar at Qualcomm, Raleigh, in February 2014.
- André Seznec presented the work on Value Prediction at Intel, Hillsboro in November 2014.
- Arthur Perais was invited to present its work on Value Prediction at the COMPASS conference, Neufchatel, April 2014, <http://compas2014.unine.ch/>.

9.3. Miscellaneous

- Erven Rohou co-advised a MSc. student at the Egypt-Japan University of Science and Technology.
- 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).
- A. Seznec was an elected member of the scientific committee of Inria till November 2014.
- A. Seznec is an elected member of the administration board of Inria since November 2014.

ATEAMS Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, scientific chair

- Jurgen Vinju: General Chair, The 7th International Conference on Software Language Engineering (SLE), Steering committee member SLE.

8.1.1.2. Member of the organizing committee

- Davy Landman: Web chair, The 7th International Conference on Software Language Engineering (SLE).
- Tijs van der Storm: Social Media Chair, The 7th International Conference on Software Language Engineering (SLE); co-organizer Belgium Netherlands Seminar on Software Evolution (BENEVOL'14), co-organizer Software Development Automation'14 (SDA'14).

8.1.2. Scientific events selection

8.1.2.1. Member of the conference program committee

- Paul Klint: WCRE/CSMR ERA 2014.
- Tijs van der Storm: SLE'14, DSLDI'14, SEMS'14, FTJP'14, TTC'14.
- Jurgen Vinju: WCRE/CSMR Tool track.

8.1.2.2. Reviewer

- Tijs van der Storm: PLDI'14.

8.1.3. Journal

8.1.3.1. Member of the editorial board

- Jan van Eijck: Editor of the Journal of Logics and their Applications.
- Paul Klint: Editor Science of Computer Programming, editor Springer LNCS Series on Services Science.
- Jurgen Vinju: co-editor ERCIM news, special issue on Software Quality.

8.1.3.2. Reviewer

- Jan van Eijck: Reviewer for ESSLLI, Journal of Semantics, Journal of Logic and Computation, Fundamenta Informaticae, Synthese, Journal of Philosophical Logic, Journal of Logic, Language and Information, Cambridge University Press.
- Tijs van der Storm: Journal of Software & Systems Modeling, Science of Computer Programming, Computer Languages, Computer Languages, Systems and Structures, Automated Software Engineering.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Jan van Eijck, "Software Testing", 6 EC, Master Programme Software Engineering, Universiteit van Amsterdam, The Netherlands.

Master: Jan van Eijck, "Functional Specification of Algorithms", 6 EC, Master Programme Logic, Universiteit van Amsterdam, The Netherlands.

Master : Tijs van der Storm, “Software Construction”, 6 EC, Universiteit van Amsterdam, The Netherlands.

8.2.2. Supervision

PhD : Jeroen van den Bos, “Gathering Evidence: Model-Driven Software Engineering in Automated Digital Forensics”, Universiteit van Amsterdam, January, 9th, 2014, Paul Klint, Tijs van der Storm.

PhD in progress : Ali Afroozeh, “Advances in GLL Parsing”, 2012, Paul Klint, Jurgen Vinju.

PhD in progress : Pablo Inostroza Valdera, “Modularity in DSL development”, 2013, Paul Klint, Tijs van der Storm.

PhD in progress : Anastasia Izmaylova, “Language Parametric Refactoring”, 2011, Paul Klint, Jurgen Vinju.

PhD in progress : Atze van der Ploeg, “Efficient Abstractions for Visualization and Interaction”, 2011, Paul Klint, Tijs van der Storm.

PhD in progress : Riemer van Rozen, “Model-Driven Game Development”, 2013, Paul Klint, Tijs van der Storm.

PhD in progress : Michael Steindorfer, “Efficient Data Structures for Meta Programming”, 2012, Paul Klint, Jurgen Vinju.

PhD in progress : Jouke Stoel, “Model Driven Infrastructure for Core Banking”, 2014, Jurgen Vinju, Tijs van der Storm.

8.2.3. Juries

Jurgen Vinju acted as reading committee member of the PhD of Maartje de Jonge, at TU Delft.

8.3. Popularization

Paul Klint:

- De Softwarerevolutie, Valedictory lecture.
- Nemo, Hoe ontstond de eerste computer?
- Nemo/Klokhuis, Hoe ontstond de eerste computer?
- BYOM: Bring Your Own Metrics (EQUA Symposium).
- The Revenge of the Coroutines (SEN Symposium).

Tijs van der Storm:

- Who’s afraid of Object Algebras?, Joy of Coding 2014.
- Hack your DSL with Rascal, CodeGeneration 2014.
- The Rascal Language Workbench, NSPyre, 2014.
- I am plain text, – resistance is futile, Sioux, 2014.
- Rascal: functional programming for source code analysis and transformation, guest lecture at Hogeschool van Arnhem en Nijmegen (HAN).

Jurgen Vinju:

- De allereerste computerprogrammeur Ada Lovelace (1815 - 1852), Kennis van NU (radio appearance).
- Complexe Software, Eindhovens Dagblad.
- De eerste programmeur, VPRO Gids.

Jan van Eijck is member of the Advisory Board (‘Raad van Advies’) of the Artificial Intelligence Curriculum, University of Groningen (since Summer 2013). Paul Klint acts as treasurer of the EAPLS and was directory of the Master Software Engineering at Universiteit van Amsterdam (UvA) until September 1, 2014. He is also board member of the Instituut voor Programmatuur en Algoritmiek (IPA). Tijs van der Storm is head of the internship committee at CWI, co-organizer of the CWI Scientific Meeting and secretary of the CWI works council.

CAIRN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Responsible of Conference Program Committee

D. Chillet was Track Chair of the 12th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC).

O. Sentieys was Track Chair at IEEE NEWCAS.

A. Tisserand is program co-chair of the 22nd IEEE Symposium on Computer Arithmetic (Lyon, 22-24 June 2015).

A. Tisserand was the program co-chair of ComPAS national conference, Conférence d'informatique en Parallélisme, Architecture et Système (Neuchâtel Suisse, 22-25 April 2014).

9.1.1.2. Member of Conference Program Committee

E. Casseau was a member of the technical program committee of SiPS.

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

M. Gautier was a member of the technical program committee of IEEE WCNC, IEEE PIMRC, IEEE ICCVE, and IARIA COCORA.

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

A. Tisserand was a member of technical program committee of DASIP, IEEE NEWCAS, IEEE PATMOS, and IEEE Reconfig.

O. Sentieys was a member of technical program committee of IEEE/ACM DATE, IEEE FPL, IEEE/ACM ICCAD, ACM ENSSys, ACM SBCCI, IFIP/IEEE VLSI-SoC, FTFC, GRETSI.

9.1.2. Journal

9.1.2.1. member of the editorial board

D. Chillet is member of the Editor Board of Journal of Real-Time Image Processing (JRTIP).

O. Sentieys is member of the editorial board of Journal of Low Power Electronics, Advances in Computer Engineering, and International Journal of Distributed Sensor Networks.

A. Tisserand is Associate Editor of IEEE Transactions on Computers. He is a member of the editorial board of the International Journal of High Performance Systems Architecture.

9.1.3. Other Scientific Responsibilities

D. Chillet is member of the Board of Directors of Grets Association.

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).

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).

A. Tisserand is co-organizer and president of scientific council of Seminar on Security of Embedded Electronic Systems (IRISA-DGA).

9.2. Seminars and Invitations

O. Berder gave an invited lecture at SENSO 2014 conference in Ecole des Mines, Gardanne, France, in October 2014.

O. Berder gave an invited lecture at Common Colloquium GDR Ondes and GDR ISIS in Telecom ParisTech, Paris, in December 2014.

A. Courtay gave an invited talk at the NASA/ESA Conference on Adaptive Hardware and Systems (AHS'14), Leicester, UK, on Dynamically Reconfigurable Embedded FPGA Systems in July 2014.

O. Sentieys gave an invited talk at the 24th International Conference on Field Programmable Logic and Applications (workshop on Self-adaptive heterogeneous many-core based on Flexible Tiles), Munich, Germany, in September 2014 on Runtime Mapping of Hardware Accelerators on the Embedded FPGA Layer.

O. Sentieys gave an invited talk at GreenDays'14 on Domain-Specific Computing Platforms: the Ultimate Energy-Efficiency of Hardware Accelerators.

O. Sentieys gave an invited lecture at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Ottawa, Canada, in January 2014 on FlexTiles: runtime mapping of hardware accelerators on 3D self-adaptive heterogeneous manycore.

A. Tisserand gave an invited lecture at the CNRS ECOFAC 2014 spring school on low power arithmetic circuits.

9.3. Teaching - Supervision - Juries

9.3.1. 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 (SISEA) and ENSSAT (M2)
- E. Casseau: high level synthesis, 12h, Master by Research (SISEA) and ENSSAT (M2)
- S. Derrien: component and system synthesis, 20h, Master by Research (MRI ISTIC) (M2)
- S. Derrien: computer architecture, 12h, ENS Cachan (L3)
- S. Derrien: computer architecture, 24h, ISTIC (L3)
- S. Derrien: introduction to operating systems, 8h, ISTIC (M1)
- S. Derrien: embedded architectures, 48h, ISTIC (M1)
- S. Derrien: high-level synthesis, 6h, ISTIC (M1)
- S. Derrien: software engineering project, 40h, ISTIC (M1)
- F. Charot: processor architecture, 25h University of Science and Technology of Hanoi (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: embedded processor architecture, 20h, ENSSAT (M1)
- D. Chillet: VHDL, 10h, ENSSAT (M1)
- D. Chillet: multimedia processor architectures, 24h, ENSSAT (M2)
- D. Chillet: advanced processor architectures, 24h, Master by Research (SISEA) and ENSSAT (M2)
- D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne and University of Occidental Brittany (UBO) (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, 37h, IUT Lannion (L1)
- C. Killian: signal processing, 36h, IUT Lannion (L2)
- C. Killian: automated measurements, 40h, IUT Lannion (L2)
- C. Killian: measurement chain, 20h, IUT Lannion (L2)
- C. Killian: embedded systems programming, 12h, IUT Lannion (L2)
- A. Kritikakou: computer architecture, 50h, ISTIC, Univ. Rennes 1 (L3)
- A. Kritikakou: operating systems, 24h, ISTIC, Univ. Rennes 1 (L3)
- 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 (SISEA) and ENSSAT (M2)
- P. Scalart: parametric modelisation, optimal and adaptive filters, 24h, Master by Research (SISEA) and ENSSAT (M2)
- P. Scalart: source coding, 14h, Master by Research (SISEA) 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 (SISEA) (M2)
- A. Tisserand: hardware computer arithmetic operators, 6h, Master by Research (SISEA) (M2)
- B. Vrigneau: electronics, 36h, IUT Lannion (L1)
- B. Vrigneau: telecommunications, 128h, IUT Lannion (L1)
- B. Vrigneau: digital communications, 28h, IUT Lannion (L1)
- C. Wolinski: computer architectures, 92h, 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)

9.3.2. Teaching Responsibilities

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 by Research.

D. Chillet is the responsible of the ICT Master of University of Science and Technology of Hanoi and also co-responsible of the "Embedded Systems" speciality of this master.

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.

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).

9.3.3. Supervision

PhD: Ganda-Stéphane Ouedraogo, Automatic Synthesis of Hardware Accelerator from High-Level Specifications in Flexible Radios, Univ. Rennes 1, Dec. 2014, M. Gautier, O. Sentieys

PhD: Aymen Chakhari, Analytical Accuracy Evaluation in Fixed-Point Digital Communication Systems, Oct. 2014, R. Rocher, P. Scalart.

PhD: Amine Didioui, Energy-Aware Transceiver for Energy Harvesting Wireless Sensor Networks, Oct. 2014, O. Sentieys, C. Bernier.

PhD: Matthieu Texier, Dynamic Parallelism Management in Multi-Core Architectures for Mobile Systems, Dec. 2014, O. Sentieys, C. Bernier.

PhD: Trong-Nhan Le, Global Power Management System for Self-Powered Autonomous Wireless Sensor Nodes, Jul. 2014, O. Sentieys, O. Berder.

PhD: Karim Bigou, RNS Hardware Units for ECC, Nov. 2014, A. Tisserand.

PhD: Pramod P. Udupa, Low Complexity, Parallel Algorithms and Scalable Architectures for Real Time Coherent Optical OFDM Systems, Jun. 2014, O. Sentieys.

PhD in progress: Faycal Ait Aoudia, Power Manager Design and Implementation for Wake-Up Radio WSN Nodes, Oct. 2014, O. Berder, M. Gautier.

PhD in progress: Benjamin Barrois, Approximate Computing: a New Paradigm for Energy-Efficient Computing Architectures, Oct. 2014, 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: Franck Bucheron, Secure Virtualization for Embedded Systems, Oct. 2011, A. Tisserand.

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

PhD in progress: Gabriel Gallin, Hardware Arithmetic Units and Crypto-Processor for Hyperelliptic Curves Cryptography, Oct. 2014, A. Tisserand, N. Veyrat-Charvillon.

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

PhD in progress: Jiating, Luo, Communication protocol exploration in the context of 3D integration of multiprocessors interconnected by Optical Network-on-Chip with energy constraints, Nov. 2014, D. Chillet, C. Killian, S. Le-Beux.

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

PhD in progress: Huu-Van-Long Nguyen, Design and error analysis of robust arithmetic operators for unreliable technologies, Oct. 2014, E. Casseau, A. Tisserand.

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.

PhD in progress: Van Dung Pham, Design space exploration in the context of 3D integration of multiprocessors interconnected by Optical Network-on-Chip, Dec 2014, O. Sentieys, D. Chillet, C. Killian, S. Le-Beux.

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: Baptiste Roux, Architectural Exploration of a Low-Power Flexible Radio Embedded on Drones, Oct. 2014, O. Sentieys, M. Gautier.

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

CAMUS Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

Cédric Bastoul has been co-organizing the HIP3ES 2015 workshop (High Performance Energy Efficient Embedded Systems) held in conjunction with the international conference HiPEAC 2015.

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

Philippe Clauss, Cédric Bastoul and Vincent Loechner have been part of the program committee of IMPACT 2014 (International Workshop on Polyhedral Compilation Techniques), held in conjunction with the international conferences HiPEAC 2014. Philippe Clauss, and Vincent Loechner have been part of the program committee of IMPACT 2015, held in conjunction with HiPEAC 2015.

Vincent Loechner and Cédric Bastoul have been part of the program committee of HIP3ES 2015 workshop (High Performance Energy Efficient Embedded Systems), held in conjunction with the international conference HiPEAC 2015.

Cédric Bastoul has been part of the program committee of PARMA+DITAM 2015 (6th Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures 4th Workshop on Design Tools and Architectures for Multicore Embedded Computing Platforms), held in conjunction with HiPEAC 2015.

9.1.2.2. reviewer

Vincent Loechner has been reviewer for the IMPACT 2015 workshop.

Philippe Clauss has been reviewer for the following conferences: ISMM '14 (International Symposium on Memory Management), IMPACT 2015.

Cédric Bastoul has been reviewer for the following conferences: CGO 2014 (International Conference on Code Generation and Optimization), PARMA 2014 and 2015 (International Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures), IMPACT 2014 (International Workshop on Polyhedral Compilation Techniques), HIP3ES 2015 (International Workshop on High Performance Energy Efficient Embedded Systems).

9.1.3. Journal

9.1.3.1. reviewer

Philippe Clauss has been reviewer for the following journals: IEEE Transactions on Computers, ACM Transactions on Programming Languages and Systems (TOPLAS), ACM Transactions on Architecture and Code Optimization (TACO), IEEE Transactions on Parallel and Distributed Systems (TPDS).

Cédric Bastoul has been reviewer for the following journals: Journal of Parallel and Distributed Computing (JPDC), ACM Transactions on Architecture and Code Optimization (TACO), Parallel Computing (ParCo).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Philippe Clauss and Alain Ketterlin did not teach during the first semester of 2014 since they were detached at Inria (*délégation*).

Licence : Vincent Loechner, Operating Systems, 38h, L2, Strasbourg University, France
 Master : Vincent Loechner, Python Programming, 38h, M1, Strasbourg University, France
 Master : Vincent Loechner, Parallelism, 15h, M1, Strasbourg University, France
 Master : Vincent Loechner, Parallel Programming, 32h, M1, Strasbourg University, France
 Master : Vincent Loechner, Parallel Programming, 30h, M2, Strasbourg University, France
 Master : Vincent Loechner, Advanced compilation, 8h, M1, Strasbourg University, France
 Master : Vincent Loechner, Embedded Systems, 32h, M2, Strasbourg University, France
 Master : Vincent Loechner, Real-time Programming, 22h, M1, Strasbourg University, France
 Licence : Philippe Clauss, Computer Architecture, 45h, L2, Strasbourg University, France
 Master : Philippe Clauss, Compilation, 78h, M1, Strasbourg University, France
 Licence : Cédric Bastoul, System Programming, 49h, L2, Strasbourg University, France
 Master : Cédric Bastoul, Compiler Design, 48h, M1, Strasbourg University, France
 Master : Cédric Bastoul, Advanced compilation, 29h, M1, Strasbourg University, France
 Master : Cédric Bastoul, Parallelism, 20h, M2, Strasbourg University, France
 Master : Cédric Bastoul, Introduction to Research, 7h, M1, Strasbourg University, France
 Licence : Éric Violard, Functional Programming, 42h, L2, Strasbourg University, France
 Licence : Éric Violard, Computer Architectures, 23h, L2, Strasbourg University, France
 Licence : Éric Violard, Algorithms and Data Structures, 34h, L2, Strasbourg University, France
 Master : Éric Violard, Compiler Design, 54h, M1, Strasbourg University, France
 Master : Éric Violard, Semantics, 48h, M1, Strasbourg University, France
 Master : Éric Violard, Introduction to Research, 6h, M1, Strasbourg University, France
 Licence : Alain Ketterlin, Computer Networks, 66h, L3, Strasbourg University, France
 Licence : Alain Ketterlin, Algorithms and Data Structures, 40h, L3, 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 Martínez 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

PhD in progress : Yann Barsamian, A Parallel Programming Environment based on the Xfor Control Structure, October 2014, Éric Violard

9.2.3. Juries

Philippe Clauss participated to the following PhD juries in 2014:

Date	Candidate	Place	Role
Sept. 22	Michael KRUSE	Univ. Paris Sud	Reviewer
June 20	Pierre ESTERIE	Univ. Paris Sud	Reviewer

Cédric Bastoul participated to the following PhD juries in 2014:

Date	Candidate	Place	Role
November 19	Rachid Habel	École des Mines de Paris	Reviewer

9.3. Popularization

Cédric Bastoul participated to the event *Kids University* at the University of Strasbourg in November 2014

Cédric Bastoul prepared activities for *Fête de la Science* at University of Paris-Sud in October 2014

COMPSYS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organization

9.1.1.1. general chair, scientific chair

Laure Gonnord is co-chair of the “Compilation french community”, with Florian Frandner (ENSTA) and Fabrice Rastello (Inria Corse).

9.1.1.2. member of the organizing committee

Alain Darte was part of the organization (mainly by Lionel Morel, from Insa-Lyon) of the thematic day on the “compilation and execution of streaming programs” in April 2014, see Section 8.1.2 .

9.1.2. Scientific events selection

9.1.2.1. responsible of the conference program committee

Alain Darte was program chair of the topic E2 “compilers for Embedded Systems” of the international conference DATE’15 (see <http://www.date-conference.com/group/tpc/members#E>), with Rodric Rabbah (IBM), and program chair of the international workshop IMPACT’15 (see <http://impact.gforge.inria.fr/impact2015/>), with Alexandra Jimborean (Uppsala Univ.).

9.1.2.2. member of the conference program committee

Paul Feautrier was a member of the program committees of the conferences and workshops PECCS’15, PARCO’15, IMPACT’14, and IMPACT’15. Laure Gonnord was a member of the program committee of the WST’14 workshop. Tomofumi Yuki was a member of the program committee of the IMPACT’15 workshop. Alain Darte was member of the program committees of the conferences and workshops IPDPS’14, DATE’14, DATE’15, IMPACT’14, and IMPACT’15.

9.1.2.3. reviewer

In 2014, Christophe Alias has reviewed papers for DATE’15 and MEMOCODE’14. Laure Gonnord has reviewed papers for WST’14, TASE’14, VMCAI’15, and MEMOCODE’14. Tomofumi Yuki has reviewed papers for IMPACT’15. Alain Darte has reviewed papers for MICRO-47 (2014), DATE’15, and IMPACT’15.

9.1.3. Journal

9.1.3.1. member of the editorial board

Paul Feautrier is a member of the editorial board of the journals “International Journal of Parallel Programming” and “Parallel Computing”.

9.1.3.2. reviewer

In 2014, Christophe Alias has reviewed papers for ACM TACO (Transactions on Architecture and Code Optimization) and Elsevier IPL (Information Processing Letters). Paul Feautrier has reviewed papers for ACM TOPLAS (Transactions on Programming Languages and Systems) and ACM TODAES (Transactions on Design Automation of Electronic Systems). Tomofumi Yuki has reviewed papers for ACM TOPLAS and ACM TACO. Alain Darte has reviewed papers for ACM TACO and IEEE Transactions on Computers.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

- Christophe Alias: Introduction à la compilation, L3, INSA Centre-Val-de-Loire: Spring 2014 (CM+TD=18h).
- Christophe Alias: Architecture des ordinateurs, L2, Université Lyon 1 Claude Bernard: Spring 2014 (TP=15h).
- Christophe Alias: Concours E3A, épreuve informatique MPSI (shepherding/exams): Spring 2014.
- Laure Gonnord: Architecture des ordinateurs, L2, Université Lyon 1 Claude Bernard: Spring 2014 (TD+TP=40h), and Autumn 2014 (Course+TD 40h).

Master:

- Christophe Alias, Compilation avancée (CM 10h), M2, Ecole Normale Supérieure de Lyon.
- Christophe Alias, Compilation (CM 24h), M1, Ecole Normale Supérieure de Lyon.
- Laure Gonnord, Introduction aux systèmes et réseaux (CM/TP 52h), M2 Pro, Université Lyon 1.
- Laure Gonnord, Compilation (TD/TP 24h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord, Complexité (TD 15h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord, Temps réel (TP 24h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord also organized two research schools (24h each) for the M1-ENS students. In 2014, the topic was “Programming embedded systems with synchronous languages” (invited speakers: Julien Forget, Abdoulaye Gamatié, Alain Girault, Nicolas Halbwachs). In 2015, the topic will be “Static analyses in the state-of-the-art compilers” (invited speaker: Fernando Pereira).

E-learning:

- Paul Feautrier has recorded a lecture on the polyhedral model, to be part of a course on auto-parallelization sponsored by the IEEE Computer Society (University of Illinois at Urbana-Champaign, Sept. 5-7) and organized by Hironori Kasahara and David Padua.
- Following the 2013 Spring School on Polyhedral Code Analysis and Optimization organized by Alain Darté, the videos of most courses have been collected and made available in 2014 (see <http://labexcompilation.ens-lyon.fr/polyhedral-school/videos/>). See also Section 8.4.1.2 .

9.2.2. Supervision

- PhD in progress: Guillaume Iooss, “Semantic tiling”, started in September 2011, joint PhD ENS-Lyon/Colorado State University, advisors: Christophe Alias and Alain Darté (ENS-Lyon) / Sanjay Rajopadhye (Colorado State University).
- PhD in progress: Alexandre Isoard, “Streaming-related code optimizations”, started in September 2012, advisor: Alain Darté.
- PhD in progress: Maroua Maleej, “Low cost static analyses for compilers”, started in October 2014, advisors: Laure Gonnord and Alain Darté.

9.2.3. Juries

Paul Feautrier was a member of the PhD defense committees of Michael Kruse (Orsay, Sept. 26, 2014), entitled “Lattice QCD Optimization and Polytopic Representations of Distributed Memory”, and of Luc Michel (Grenoble, Dec. 18, 2014), entitled “Contributions à la traduction binaire dynamique: support du parallélisme d’instructions et génération de traducteurs optimisés”.

Laure Gonnord was a reviewer for the PhD thesis of Chan N'Go (Rennes, Jul. 2014), entitled "Formal Verification of a Synchronous Data-flow Compiler: From Signal to C".

Alain Darté was member of the PhD defense committee of Romain Brillu (Nantes, Nov. 12, 2014), entitled "Efficient Design and Programming of MPSoC (Multiple Processors System on Chip) Architectures".

9.3. Popularization

- Alain Darté was invited to give a long keynote (1h30), as an introduction to polyhedral techniques ("Polyhedral optimizations? Not even scared!" [2]), to the spanish Conference Jornadas Sarteco, the equivalent of the french COMPAS conference, see <http://www.jornadassarteco.org/transparencias-de-las-charlas-invitas/>.
- In Sep. 2014, together with ten other specialists in automatic parallelization, Paul Feautrier recorded a lecture on the "polyhedral model" for a video course on automatic parallelization to be published by the IEEE.
- Paul Feautrier's 1988 "Array Expansion" seminal paper has been selected for the 25th Anniversary Volume of the ACM International Conference on Supercomputing, with 34 other papers, among 1800 papers published from 1987 to 2011. A short "reminescence" paper [13] has been written for the occasion. <http://dl.acm.org/citation.cfm?doid=2591635.2591641>.
- Alain Darté participated to the "Refresh" Inria Rhône-Alpes initiative, for improving the scientific life of the Inria regional center, as well as to the working group on "team management".

DREAMPAL Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. member of the organizing committee

F. Guyomarch, P. Marquet and S. Meftali are members of the ComPAS organizing committee. This conference will take place in Lille in 2015.

F. Guyomarch and S. Meftali are members of the Archi organizing committee. This summer school will take place in Lille in 2015.

R. Ben Atitallah is a member of the Green Days@Rennes organizing committee. The scientific event was held in Rennes, July 2014.

8.1.2. Scientific events selection

8.1.2.1. responsable of the conference program committee

S. Meftali is responsable of the ComPAS conference program committee. This conference will take place in Lille in 2015.

8.1.2.2. member of the conference program committee

F. Guyomarch is a member of the ComPAS program committee.

V. Rusu is a member of the WRLA2014 program committee.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Philippe Marquet, Introduction to Computer Science, 15h, Secondary Education Teacher 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 : Samy Meftali, Architecture des ordinateurs, 75h, L2, UFR IEEA, Université Lille 1, France

Licence : Samy Meftali, Programmation du matériel, 40h, L3, UFR IEEA, Université Lille 1, France

Master: Samy Meftali, Architectures évoluées des ordinateurs, 80h, M1, UFR IEEA, Université Lille 1, France

Master: Samy Meftali, Vérification des SoC, 16h, M2, UFR IEEA, Université Lille 1, France

Licence : Jean-Luc Dekeyser, Architecture des ordinateurs, 80h, L2, UFR IEEA, Université Lille 1, France

Master: Jean-Luc Dekeyser, Architectures évoluées des ordinateurs, 105h, M1, UFR IEEA, Université Lille 1, France

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

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

Licence : F. Guyomarch, Modélisation mathématique, 28h, L2, IUT-A (Univ. Lille 1)

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 : V. Rusu, Architecture avancée des ordinateurs, 42h, M1, UFR IEEA, (Univ. Lille 1)

Master : V. Rusu, Spécification et vérification de logiciels , 27h, M1, UFR IEEA, (Univ. Lille 1)

8.2.2. Supervision

PhD : A. Arusoae, *A Generic Framework for to Symbolic Execution*, Univ. Iasi (Romania), Sept 2014. Supervisors: D. Lucanu, V. Rusu.

PhD in progress : H. Krichene, *SCAC : Modèle d'exécution générique faiblement couplé pour les architectures massivement parallèle sur puce*, March 2011, Philippe Marquet & Jean-Luc Dekeyser

PhD in progress : W. Chouchene, *Partial reconfiguration model for dynamic and massively parallel architecture : towards 3D FPGAs*, 01/10/2013, Jean-Luc Dekeyser, Rabie Ben Atitallah and Samy Meftali

PhD in progress : K. Ali, *Massively parallel dynamically reconfigurable architecture for real-time vidéo processing applications*, 01/10/2013, Jean-Luc Dekeyser, Rabie Ben Atitallah

PhD in progress : V. Viswanathan, *Parallel and Dynamic reconfigurable computing system*, 01/02/2012, Jean-Luc Dekeyser and Rabie Ben Atitallah

PhD in progress : V. Craciun, *Hardware monitoring*, Sept 2014, F. Guyomarch and D. Lucanu.

8.2.3. Juries

Doctorat de Amel Khiar, Virtualisation des communications au sein d'une plateforme hétérogène et reconfigurable dynamiquement, Université de Cergy Pontoise, 5 novembre 2014, Samy Meftali (examineur).

Doctorat de Feriel Ben Abdallah, Modeling and Formal Verification of Power Management for the Design of Systems-on-Chip, Université de Valenciennes, 12 décembre 2014, Samy Meftali (examineur).

8.3. Popularization

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

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

He organizes and participates to the visit of classrooms on the Inria Plateau at EuraTechnologies, promoting interactions between the scientific community and secondary school students and their teachers. He organizes and/or animates events with children and/or adults in order to initiate them to code via Scratch or to computer science via unplugged activities (Poitiers, February 2014; Paris, October 2014; Inria Lille, December 2014).

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.

Hana Krichene participated in a contest "my thesis in 180 seconds", March 2014 - University Lille 1. The aim of the competition is to present the PhD student researches in simple terms in 3 minutes, with a clear, concise and convincing presentation to a diverse audience.

GCG Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

- Fabrice Rastello: Publication chair ACM/IEEE CGO 2015
- Fabrice Rastello: Steering committee Journées française de la compilation

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committee

- Fabrice Rastello: ACM/IEEE CGO 2014, ACM/IEEE CGO 2015

9.1.2.2. Reviewer

- Fabrice Rastello: Springer CC 2014

9.1.3. Journal

9.1.3.1. Reviewer

- Fabrice Rastello: ACM TACO, Elsevier ParCo

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Fabrice Rastello (external intervention), Programming Languages and Compiler Design, 4.5 hours, M1 of international MoSIG, UJF, Grenoble, France

Master : Fabrice Rastello (with Christophe Alias and Florent de Dinechin), Advanced Compilation, 15 hours, M1/M2, ENS Lyon, France

Post-doctoral : Fabrice Rastello, SSA based compiler design, 6 hours, CRI, Yaounde Cameroun

9.2.2. Supervision

- PhD in progress: Duco van Amstel, Scheduling and optimization for memory locality of dataflow programs on many-core processors, April 1st 2013, advised by Fabrice Rastello and Benoit Dupont-de-Dinechin
- PhD in progress: Diogo Sampaio, Profiling Guided Hybrid Compilation, October 8 2013, advised by Fabrice Rastello
- PhD in progress: François Gindraud, Semantics and compilation for a data-flow model with a global address space and software cache coherency, January 1st 2013, advised by Fabrice Rastello and Albert Cohen.
- PhD in progress: Venmugil Elango, Dynamic Analysis for Characterization of Data Locality Potential, September 2010, advised by Fabrice Rastello and P. Sadayappan.

9.2.3. Juries

- Feng Li, Reviewer, 20th of Mai, Compiling for a multithreaded dataflow architecture: algorithms, tools, and experience, Doctorat de l'UPMC EDITE
- Kevin Pouget, Jury, 3rd of February, Programming-Model Centric Debugging for Multicore Embedded Systems, MSTII, Grenoble

PAREO Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

8.1.1.1. Conference program committee membership

Horatiu Cirstea:

- PC member of RuleML 2014 (International RuleML Symposium on Rule Interchange and Applications).
- Steering committee of RULE.

Sergueï Lenglet:

- PC member of WPTE'14 (Workshop on Rewriting Techniques for Program Transformations and Evaluation)

Pierre-Etienne Moreau:

- PC member of TERMGRAPH'2014 (8th International Workshop on Computing with Terms and Graphs)
- PC member of WRLA'2014 (10th International Workshop on Rewriting Logic and its Applications)

Sorin Stratulat:

- PC member of CISIS 2014 (7th International Conference on Computational Intelligence in Security for Information Systems)
- PC member of IAS 2014 (10th International Conference on Information Assurance and Security)
- PC member of SYNASC 2014 (16th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing)

8.1.1.2. Reviewing activities

Horatiu Cirstea:

- Reviewer for ESOP'2014, ICTAC'2014, LOPSTR'2014

Sergueï Lenglet:

- Reviewer for CSL-LICS'2014, RTA-TLCA'2014, FOSSACS'2015

Pierre-Etienne Moreau:

- Reviewer for TERMGRAPH'2014, WASDETT'2014

8.1.2. Journal

8.1.2.1. Editorial board membership

Pierre-Etienne Moreau:

- Advisory Board of Science of Computer Programming, software track

8.1.2.2. Reviewing activities

Horatiu Cirstea:

- Reviewer for Journal of Symbolic Computation

Sergueï Lenglet:

- Reviewer for Fundamenta Informaticae and HOSC (Higher-Order and Symbolic Computation)

Pierre-Etienne Moreau:

- Reviewer for Electronic Proceedings in Theoretical Computer Science (EPTCS)

Sorin Stratulat:

- Reviewer for Journal of Symbolic Computation

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: Sergueï Lenglet, teaching at IUT Charlemagne, first year and second year students.

Licence: Horatiu Cirstea, Responsible for the first year of the Licence in Computer Science, Université de Lorraine.

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.

Master: Horatiu Cirstea, Responsible for the Master speciality “Logiciels: Théorie, méthodes et ingénierie”, Université de Lorraine.

Master: Pierre-Etienne Moreau, Head of the Computer Science Department at Mines Nancy, Université de Lorraine.

Doctorate: Pierre-Etienne Moreau, Implementing Term Rewriting, International School on Rewriting, Valparaíso, Chile.

8.2.2. Supervision

PhD: Jean-Christophe Bach, A formal Island for qualifiable model transformations, Université de Lorraine, September 12th 2014, Pierre-Etienne Moreau

PhD in progress: Duy Duc Nguyen, Aided design of multi-physics and multi-scale systems based on asymptotic methods, Horatiu Cirstea (co-supervised with Michel Lenczner and Federic Zamkotsian)

PhD in progress: Amira Henaïen, Certification du raisonnement formel porté sur des systèmes d’information critiques, November 2010, Sorin Stratulat (co-supervised with Maurice Margenstern)

8.2.3. Juries

Horatiu Cirstea:

PhD committee of Julien Ferté, reviewer, “Régularité et contraintes de descendance, équations algébriques+”, Marseille 2014

PhD committee of Hernan Vanzetto, examiner, “Automatisation des preuves et synthèse des types pour la théorie des ensembles dans le contexte de TLA+”, Nancy 2014

PhD committee of Bin Yang, reviewer, “Contribution to a kernel of a symbolic asymptotic modeling software”, Besançon 2014

Pierre-Etienne Moreau:

PhD committee of Jean-Christophe Bach, supervisor, “Un îlot formel pour les transformations de modèles qualifiables”, Nancy 2014

PhD committee of Faiez Zalila, reviewer, “Methods and Tools for the Integration of Formal Verification in Domain-Specific Languages”, Toulouse 2014

PhD committee of Cyrille Wiedling, examiner, “Formal Verification of Advanced Families of Security Protocols: E-Voting and APIs”, Nancy 2014

Sorin Stratulat:

PhD committee of Abdelkader Kersani, examiner, “Preuves par induction dans le calcul de superposition”, Grenoble 2014

8.3. Popularization

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.

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. He 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.

Pierre-Etienne Moreau is member of the national committee for Inria “Médiation Scientifique”. He also participated to “Fête de la Science 2014” at Mines Nancy.

POSTALE Team

8. Dissemination

8.1. Promoting Scientific Activities

Marc Baboulin Member of Steering Committee of ACM High Performance Computing Symposium (HPC'14), Tampa, Florida, April 13-16, 2014.

Marc Baboulin organizer of the workshop "Linear least squares and applications", 19th International Linear Algebra Society Conference (ILAS 2014), Seoul, South Korea, Aug. 06-09, 2014.

Marc Baboulin organizer of the minisymposium "Randomized algorithms in parallel matrix computations" at the SIAM Conference on Parallel Processing for Scientific Computing, Portland (OR), USA, Feb. 18-21, 2014.

Christine Eisenbeis IJPP (International Journal on Parallel Programming) editorial board.

Christine Eisenbeis comité d'organisation du colloque "Recherche et démocratie", 21-22 mai 2014, Orsay, (<http://www.centre-dalembert.u-psud.fr/archives-colloques/2014-recherche-scientifique-et-democratie/>).

Christine Eisenbeis 5th Workshop on applications for multi-core architectures, October 22-23, 2014, University Pierre et Marie Curie, Paris, France

Joël Falcou Membre du comité français de normalisation des langages C et C++ (JTC1/SC22/WG21) auprès de l'AFNOR depuis janvier 2011

Joël Falcou Co-chair of the C++NOW conference on C++ <http://cppnow.org/>

Joël Falcou Organizer and co-chair of the 2014 Workshop on Programming Models for SIMD/Vector Processing <https://sites.google.com/site/wpmvp2014/home>

Joël Falcou Membre fondateur du *User Group C++ francophone* (<http://www.meetup.com/User-Group-Cpp-Francophone/>)

Lionel Lacassagne reviewer for JRTIP and Eurasip Signal journals

Lionel Lacassagne co-chairman of the "Visual Scene Analysis on Hybrid Multicore" special session at DASIP 2014.

Lionel Lacassagne Program Committee member of DASIP 2014.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Christine Eisenbeis, coordinatrice du module "Optimisations et compilation" du M2 recherche NSI ("Nouveaux systèmes informatiques") de l'université Paris-Sud 11. 3 heures de cours.

Master: M. Baboulin and J. Falcou teach in "Calcul Haute Performance" of M2 recherche NSI of University Paris Sud 11.

Lionel Lacassagne: Master 2 Research "Nouveau Systemes Informatique" (NSI) and Master 2 "Systemes Embarqués et Traitement de l'Information" (SETI). Computer Architecture: optimisations for multicore and SIMD processors.

Polytech 5th year: M. Baboulin and J. Falcou teach the "Parallel Computing" class.

8.2.2. Supervision

PhD in progress: Ian Masliah, Automatic code generation in high-performance computing numerical libraries, University Paris Sud 11, Supervisors: M. Baboulin and J. Falcou

PhD in progress: Antoine Tran Tan, Automatic task-based code generation by C++ meta-programming, University Paris-Sud 11, Supervisor: Joël Falcou

PhD in progress: Adrien Rémy, Solving dense linear systems on accelerated multicore architectures, University Paris Sud 11, Supervisors: M. Baboulin and B. Rozoy

PhD in progress: Yushan Wang, Numerical simulations of incompressible fluid flows on heterogeneous parallel architectures, University Paris Sud 11, Supervisors: M. Baboulin and O. Le Maître

PhD in progress: Lénaïc Bagnères, université Paris-Sud 11, supervisors: Cédric Bastoul and Christine Eisenbeis

PhD defended, december 2014: Alessandro Leite, université Paris-Sud 11, supervisors: Alba de Melo (university of Brazilia), Claude Tadonki (CRI, école des Mines de Paris), Christine Eisenbeis

PhD defended, september 2014, Michael Kruse, Polytopic memory layout optimization, université Paris-Sud 11, supervisor: Christine Eisenbeis

PhD in progress: Jason Lambert, Interactive Non-Destructive Testing algorithm on SIMD multicore processors and GPU. CEA List/Disc funding, université Paris-Sud 11, supervisor: Lionel Lacassagne

8.2.3. Juries

- Marc Baboulin, Thèse de Viviana Siless (08/07/2014). Fonction exercée: président du jury
- Marc Baboulin, HDR de Christophe Denis (04/07/2014). Fonction exercée: rapporteur
- Marc Baboulin, Thèse de Jesus Camacho Rodriguez (25/09/2014). Fonction exercée: président du jury
- Marc Baboulin, HDR de Sylvie Boldo (06/10/2014). Fonction exercée: président du jury
- Marc Baboulin, Thèse de Philippe Théveny (31/10/2014). Fonction exercée: président du jury
- Marc Baboulin, Thèse de Vincent Reverdy (12/11/2014). Fonction exercée: examinateur
- Christine Eisenbeis, membre du jury de la thèse de Michael Kruse, "Lattice QCD Optimization and Polytopic Representations of Distributed Memory", vendredi 26 septembre 2014, université Paris-Sud
- Christine Eisenbeis, membre du jury de la thèse de Alessandro Ferreira Leite, "A User-Centered and Autonomic Multi-Cloud Architecture for High Performance Computing Applications", mardi 2 décembre 2014, université Paris-Sud
- Lionel Lacassagne, membre du jury de la thèse de Haixiong Ye, "Impact of High Level Transforms on High Level Synthesis: application to signal and image processing", ST Microelectronics funding, 20 mai 2014, université Paris-Sud

8.3. Popularization

Christine Eisenbeis est membre du conseil scientifique des programmes du centre d'Alembert, Centre Interdisciplinaire d'Étude de l'Évolution des Idées, des Sciences et des Techniques (CIEEIST), de l'université Paris-Sud. À ce titre, elle a fait partie du comité d'organisation du colloque "Recherche et démocratie", 21-22 mai 2014, Orsay, (<http://www.centre-dalembert.u-psud.fr/archives-colloques/2014-recherche-scientifique-et-democratie/>). Lors de l'animation "Livres au marché" de Malakoff, le 23 novembre 2014, elle a présenté, avec Jean-Pierre Archambault, le livre d'enseignement en terminale de l'ISN (Informatique et Sciences du Numérique) (principal auteur Gilles Dowek).

TASC Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

- **Gilles Chabert**: Organization of a workshop on constraints, intervals and geometry in Mine de Nantes on June 2014 (<http://ibex-lib.org/workshop-23-06-14>).
- **Éric Monfroy**: Co-chair of the **ACM SAC CSP**. tracks 2014 and 2015.
- **Thierry Petit**: Chairman of the 10th Edition of JFPC conference, June 11-13 2014, Angers, **JFPC 2014**.

9.1.1.2. member of the organizing committee

- **Éric Monfroy**: Member of the organizing committee of **JFPC 2014**.

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

- **Nicolas Beldiceanu**: Member of the senior program committee of **CP 2014**.
- **Nicolas Beldiceanu**: Member of the program committee of **CPAIOR 2014**.
- **Nicolas Beldiceanu**: Member of the program committee of **CPAIOR 2015**.
- **Nicolas Beldiceanu**: Member of the program committee of **IJCAI 2015**.
- **Xavier Lorca**: Member of the program committee of JFPC 2015 (in Bordeaux).
- **Xavier Lorca**: Member of the program committee of **IJCAI 2015**.
- **Éric Monfroy**: Member of the program committee of **EvoCOP 2015**.
- **Thierry Petit**: Member of the program committee of **CPAIOR 2014**.
- **Thierry Petit**: Member of the program committee of **IEEE-ICTAI 2014** (Special track on SAT-CSP).
- **Thierry Petit**: Member of the program committee of **ECAI 2014**.
- **Charles Prud'homme**: Member of the program committee of **JFPC 2014**.
- **Florian Richoux**: Member of the Program Committee of **LION 9**.
- **Florian Richoux**: Member of the Program Committee of **SAC 15**.
- **Florian Richoux**: Member of the program committee of **JFPC 2014**.
- **Charlotte Truchet**: Member of the program committee of **ParSearchOpt 2014**.
- **Charlotte Truchet**: Member of the program committee of **JFPC 2014**.

9.1.2.2. reviewer

- **Nicolas Beldiceanu** reviewer at **AAAI 2014**.
- **Gilles Chabert** reviewer at **SIAM Journal of Scientific Computing**.

9.1.3. Journal

9.1.3.1. member of the editorial board

- **Nicolas Beldiceanu**, **Constraints** (Springer).
- **Thierry Petit**, **Constraints** (Springer).
- **Florian Richoux**, **Encyclopedia of Computer Graphics and Games** (Springer).

9.1.3.2. reviewer

- **Xavier Lorca**: Reviewer for **Constraints (Springer)**.
- **Éric Monfroy**: Reviewer for IEEE TEC (Elsevier).
- **Éric Monfroy**: Reviewer for Information Sciences (Elsevier).
- **Florian Richoux** reviewer at **journal IEEE Transactions on Computational Intelligence and AI in games**.
- **Florian Richoux** reviewer at **Annals of Mathematics and Artificial Intelligence, Springer**.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master: **Nicolas Beldiceanu**, Constraint (**Master ORO**), 30h, M2, Nantes University, France.
- Master: **Nicolas Beldiceanu**, Logic Programming, 32h, M2, Mines Nantes, France.
- Master: **Nicolas Beldiceanu**, Gipad end project, 8h, M2, Mines Nantes, France.
- Licence: **Nicolas Beldiceanu**, Programming with Java, 42h, L3, Mines Nantes, France.
- Licence: **Nicolas Beldiceanu**, IPIPIP project, 12h, L1, Mines Nantes, France.
- Master: **Gilles Chabert**, Non-linear programming, 20h, M2, Mines Nantes, France.
- Master: **Gilles Chabert**, Non-linear optimization, 20h, M1, Mines Nantes, France.
- Master: **Gilles Chabert**, Non-linear optimization, 24h, M1, Nantes University, France.
- Licence: **Gilles Chabert**, Variational calculus, 12h, L3, Mines Nantes, France.
- Licence: **Gilles Chabert**, Numerical methods, 21h, L3, Mines Nantes, France.
- Licence: **Gilles Chabert**, Numerical methods, 15h, L3, Mines Nantes, France.
- Licence: **Gilles Chabert**, Supervisions of projects, 66h, L3, Mines Nantes, France.
- Gilles Chabert**, Member of the selection committee for a position of associate professor at **ISTIA** (Angers University).
- Master: **Xavier Lorca**, Head of the major of the Master in Engineering, Computer Science for Decision Support, M2, Mines Nantes, France.
- Master: **Xavier Lorca**, Graph Theory, Algorithms, 22h, M1, Mines Nantes, France.
- Master: **Xavier Lorca**, Artificial Intelligence and Constraint Programming, 22h, M2, Mines Nantes, France.
- Master: **Xavier Lorca**, IT System and Software Development, 45h, M2, Mines Nantes, France.
- Master: **Xavier Lorca**, Decision support systems, 45, M2, Mines Nantes, France.
- Master: **Xavier Lorca**, Supervisions of projects, L2, M1, M3, Mines Nantes, France.
- Licence: **Éric Monfroy**, Responsible of the L2 in Computer Science, Nantes University, France.
- Licence and Master: **Éric Monfroy**, Responsible of the pole "Fondements Théoriques", CS Department, Nantes University, France.
- Licence: **Éric Monfroy**, Algorithm 2, 16h, L2, Nantes University, France.
- Licence: **Éric Monfroy**, Logic, 40h, L2, Nantes University, France.
- Licence: **Éric Monfroy**, Language theory, 96h, L3, Nantes University, France.
- Licence: **Éric Monfroy**, Computer architecture, 40h, L3, Nantes University, France.
- Master: **Éric Monfroy**, supervision of 5 M2-MIAGE students (alternants), M2, Nantes University, France.
- Master: **Éric Monfroy**, seminar about problem modelisation (ORO Master), 2, M2, Nantes University, France.

Master: **Thierry Petit**, Director of the Combinatorial Optimization degree, GIPAD, M2, Mines Nantes, France.

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

Master: **Thierry Petit**, Discrete optimization, 9h, M2, Mines Nantes, France.

Master: **Thierry Petit**, Constraint Programming in **CHOCO**, 20h, M2, Mines Nantes, France.

Licence: **Thierry Petit**, Data structures, 20h, L2, Mines Nantes, France.

Licence: **Thierry Petit**, Java Programming, 40h, L2, Mines Nantes, France.

Licence: **Thierry Petit**, HMI, 13h, L2, Mines Nantes, France.

Licence: **Thierry Petit**, FIL project supervisor, 12h, L2, Mines Nantes, France.

Licence: **Thierry Petit**, IPIPIP project, 12h, L1, Mines Nantes, France.

Licence: **Thierry Petit**, Introduction to Constraint Programming, 4h, L2, Worcester Polytechnic Institute, USA.

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

Master: **Florian Richoux**, Prediction of Parallel Speed-ups for Las Vegas Algorithms, 2h, M2, University of Tokyo, Japan.

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

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

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

Master: **Charlotte Truchet**, Local Search, 10h, M2, Mines Nantes.

E-learning

Pedagogical resources: **Nicolas Beldiceanu**, global constraint course, exercises (available in two formats: pdf and interactively on the web) M2, http://imedia.emn.fr/global_constraints_course/

9.2.2. Supervision

PhD: Bruno Belin, Interactive conception of sustainable urban environments with constraints, Nantes University, November 27, 2014, **Charlotte Truchet**, **Marc Christie**, **Frédéric Benhamou**.

PhD: Jean-Guillaume Fages, Graph Theory in Constraint Programming, Theory and application to several graph covering problems, Nantes University, October 23, 2014, **Xavier Lorca**, **Nicolas Beldiceanu**.

PhD: **Charles Prud'homme**, Controlling Propagation and Search within a Constraint Solver, Nantes University, February 28, 2014, **Xavier Lorca**, **Narendra Jussien**, **Rémi Douence**.

PhD in progress: Anicet Bart, Mixed Constraint Solving, October 2014, **Charlotte Truchet**, **Éric Monfroy**.

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

PhD in progress: Gilles Madi Wamba, Integrating time automata and constraint programming for modeling vm assignment in a data centre, October 2014, **Nicolas Beldiceanu**, **Didier Lime**, **Oliver H. Roux**.

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

PhD in progress: Nicolás Sebastián Gálvez Ramírez, CP for Software Engineering, November 2014, **Éric Monfroy**, co-tutelle with Chile also involving Carlos Castro, Frédéric Saubion.

PhD in progress: Alejandro Reyes Amaro, New parallel algorithms for combinatorial optimization, October 2013, [Florian Richoux](#), [Éric Monfroy](#).

9.2.3. Juries

- [Nicolas Beldiceanu](#), Member of the committee of the HdR of [Xavier Lorca](#), Élément de flexibilité et d'efficacité en programmation par contraintes, (Nantes University, November 6, 2014).
- [Nicolas Beldiceanu](#), Member of the committee of the HdR of [Thierry Petit](#), Concilier expressivité et efficacité en programmation par contraintes, (Nantes University, December 4, 2014).
- [Nicolas Beldiceanu](#), Member of the PhD committee of the thesis of Jean-Guillaume Fages, Graph Theory in Constraint Programming, Theory and application to several graph covering problems, (Nantes University, October 23, 2014).
- [Frédéric Benhamou](#), Member of the PhD committee of the thesis of Bruno Belin, Interactive conception of sustainable urban environments with constraints, (Nantes University, November 27, 2014).
- [Gilles Chabert](#), Member of the PhD committee of the thesis of Aymeric Bethencourt, Interval Analysis for swarm localization. Application to underwater robotics. (ENSTA Bretagne, September 30, 2014).
- [Xavier Lorca](#), Member of the PhD committee of the thesis of Jean-Guillaume Fages, Graph Theory in Constraint Programming, Theory and application to several graph covering problems, (Nantes University, October 23, 2014).
- [Xavier Lorca](#), Member of the PhD committee of the thesis of Charles Prud'homme, Controlling Propagation and Search within a Constraint Solver, (Nantes University, February 28, 2014).
- [Charlotte Truchet](#), Member of the PhD committee of the thesis of Bruno Belin, Interactive conception of sustainable urban environments with constraints, (Nantes University, November 27, 2014).
- [Éric Monfroy](#), Member of the HDR committee of the Habilitation thesis of [Xavier Lorca](#), Élément de flexibilité et d'efficacité en programmation par contraintes, (Nantes University, November 6, 2014).
- [Éric Monfroy](#), Member of the HDR committee of the Habilitation thesis of [Adrien Goeffon](#), Modèles d'abstraction pour la résolution de problèmes combinatoires, (Angers University, November 17, 2014).
- [Éric Monfroy](#), Member of the HDR committee of the Habilitation thesis of [Thierry Petit](#), Concilier expressivité et efficacité en programmation par contraintes, (Nantes University, December 4, 2014).
- [Éric Monfroy](#), Member of the PhD committee of the thesis of Xavier Dupont, (Caen University, December 18, 2014).
- [Éric Monfroy](#), Member of the Magister committee of the Magister thesis of N. Galvez, (UTFSM, Chile, November 19, 2014).

9.3. Popularization

- A user guide is now available for [CHOCO](#): 164 pages describing how to use [CHOCO](#), together with a new website, see <http://www.choco-solver.org>. The next topics on the way will include:
 - Dealing with strong consistencies.
 - Designing an even more efficient free search strategy.
 - Providing a light explanation framework.
- Within the context of the [global constraint catalog](#):
 - On-line interactive exercises completed (see http://imedia.emn.fr/global_constraints_course/).
 - Effort for providing more [TikZ](#) illustrations has been continued (about 1000 figures are currently available and 60 figures remain to be redesigned to [TikZ](#)) by [Nicolas Beldiceanu](#).

- Reorganization of the production of the pdf version (and enhancing look and navigation within the pdf) by **Mats Carlsson**.
- Update of the web version (see <http://sofdem.github.io/gccat/>) by **Sophie Demassey**.
- A strong effort has also been made in 2014 to improve the dissemination of **IBEX** and the collaboration of programmers. This includes:
 - Course on **IBEX** by **Gilles Chabert** at **MACS 2015**.
 - Creation of a new web site, see <http://www.ibex-lib.org/>.
 - Documentation writing (low-level interval arithmetic operations, contractors), see <http://www.ibex-lib.org/doc/>.
 - Migration of the code from SVN+sourceforge to github (github.com/ibex-team/ibex-lib).
 - Support via the new forum (<http://ibex-lib.org/forum>).
 - Bug/issue tracking system, private wiki for developers.
 - Introduction of Travis for continuous integration.
- Within the context of *Artificial Intelligence and real time strategy games*,
 - Interview by Inria Bretagne of **F. Richoux** on his work about Game AI, see emergences.inria.fr/emergences-2014/newsletter-n30/L30-STARCRAFT.
 - **F. Richoux** has been invited to write a short article about his work about Game AI in the “Bulletin de l’Association Française pour l’Intelligence Artificielle”. It should appear on January 2015.
- Presentation at the workshop **les femmes dans le monde académique** by **Charlotte Truchet**.
- A the 2014 edition of the Fête de la Science (Nantes University):
 - One talk on *Challenges around optimizations problems* was given by **Xavier Lorca**.
 - A session discussing and answering questions around the work of professor and researcher in computer science with young persons (18 years old) was spent by **N. Beldiceanu**.

AOSTE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

- Julien Deantoni: GeMoc'2014 (workshop) [43]
- Marie-Agnès Peraldi-Frati: CIEL'2014 [35]

9.1.2. Scientific events selection

9.1.2.1. responsible of the conference program committee

- Laurent George: PC co-chair of 19th International Conference on Reliable Software Technologie - Ada-europe'2014, and of Workshop on Mixed Criticality for Industrial Systems (WMCIS'2014)

9.1.2.2. member of conference program committee

- Robert de Simone: EmSoft'2014, FDL'2014, Memocode'2014.
- Yves Sorel: RTNS 2014, DASIP 2014, EMSOFT 2014, ADA-Europe 2014
- Dumitru Potop Butucaru: Memocode'2014, ACSOFT 2014, EsISyn 2014
- Julien Deantoni: CIEL 2014, CAL 2014.

9.1.3. Journal

9.1.3.1. member of the editorial board

Yves Sorel: Traitement du Signal Journal

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Robert de Simone, Models of Computation for Networks-on-Chips (MoCs for NoCs), 36h, M2 International, UNS.

Master: Robert de Simone, Functional and Temporal Correctness, 36h, M1 International, 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, Paris

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

Master : Julien Deantoni, Encadrement Projet en équipe, 31h, M1, Polytech'Nice

Master : Julien Deantoni, Encadrement Apprentissage, 8h, M1, Polytech'Nice

Master : Julien Deantoni, Architecture machine, 24h, niveau M1, Polytech'Nice, France.

Master : Julien Deantoni, Systèmes embarqués et Ambient, 10h, M2, Polytech'Nice, France.

Master : Julien Deantoni, Langage C++, 88h, M1, Polytech'Nice, France.

Master : Julien Deantoni, Ingénierie Dirigée par les modèles par la pratique, 24h, M2, Polytech'Nice, France.

Master : Julien Deantoni, Ingénierie Dirigée par les modèles avancée, 9h, M2 Esprit Tunis, Tunisia.

Master: Dumitru Potop Butucaru, Une approche synchrone des systèmes embarqués temps réel, 12h, M1, EPITA Paris

Master: Dumitru Potop Butucaru and Thomas Carle, L'approche synchrone de la construction des systèmes embarqués temps réel, 12h, M2, Polytech Paris UPMC.

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

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

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.

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.

9.2.2. Supervision

PhD in progress: Cristian Maxim, Probabilistic Real-Time Systems, University of UMPC-Paris-Sorbonne, co-supervised by Liliana Cucu-Grosjean with Benoit Triquet (Airbus)

PhD: Falou Ndoeye, Multiprocessor real-time scheduling taking into account preemption cost [19]; defended April 2014, supervised by Yves Sorel

PhD: Manel Djemal, *Reconciling performance and predictability on a NoC-based MPSoC using off-line scheduling techniques* [18], EDITE/UPMC, defended June 27th 2014, co-supervised by Alix Munier (UPMC/Lip6) and D. Potop-Butucaru.

PhD: Thomas Carle, *Efficient compilation of embedded control specifications with complex functional and non-functional properties* [16], EDITE/UPMC, defended Oct. 31st 2014, supervised by D. Potop-Butucaru.

PhD in progress: Salah Saidi, *Real-time scheduling for distributed simulation of numerical models*, University of UMPC-Paris-Sorbonne, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel

PhD in progress: Matias Vara-Larsen, *Toward a formal and hierarchical timed model for concurrent heterogeneous model*, UNS, 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: Yann Bondue, *Towards formal multimodal languages*, UNS, started December 2014, supervised by Julien Deantoni.

9.2.3. Juries

- Robert de Simone: PhD examiner of Mariem Abdelmoula (UNS)
- Yves Sorel: PhD examiner of Philippe Thierry (University Paris Est)
- Laurent George: PhD reviewer of Georges-Arnaud KEMAYO (ENSMA Poitiers), Vincent LEGOUT (Telecom ParisTech) and Gurulingesh RARAVI (University of Porto).
- Liliana Cucu-Grosjean: PhD reviewer of Maxime CheraMy (University of Toulouse-INSA) and Vladimir-Alexandru Paun (Ecole Polytechnique, Paris)
- Dumitru Potop Butucaru: PhD examiner of Chan Ngo (Univ. Rennes 1)

CONVECS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- G. Salaün was general chair for SEFM'2014 (*12th International Conference on Software Engineering and Formal Methods*), Grenoble, France, September 1–5, 2014.

9.1.1.2. Member of the organizing committee

- L. Ye was publicity chair for SEFM'2014. R. Abid and H. Evrard were members of the organizing committee for SEFM'2014.
- W. Serwe was publicity chair for FMICS'2014 (*19th International Workshop on Formal Methods for Industrial Critical Systems*), Florence, Italy, September 11–12, 2014.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committee

- G. Salaün was programme committee chair for SEFM'2014.
- F. Lang was programme committee chair for FMICS'2014.

9.1.2.2. Member of the conference program committee

- G. Salaün was programme committee member for GRAPHITE'2014 (*3rd Workshop on Graph Inspection and Traversal Engineering*), Grenoble, France, April 5, 2014.
- G. Salaün was programme committee member for ORCHOR'2014 (*International Workshop on Service Orchestration and Choreography for the Future Internet*), Anchorage, Alaska, June 30, 2014.
- G. Salaün was programme committee member for WWV'2014 (*International Workshop on Automated Specification and Verification of Web Systems*), Vienna, Austria, July 18, 2014.
- H. Garavel was programme committee member for SEFM'2014.
- G. Salaün was programme committee member for FOCLASA'2014 (*13th International Workshop on Foundations of Coordination Languages and Self-Adaptive Systems*), Rome, Italy, September 6, 2014.
- G. Salaün was programme committee member for FACS'2014 (*11th International Symposium on Formal Aspects of Component Software*), Bertinoro, Italy, September 10–12, 2014.
- R. Mateescu and W. Serwe were programme committee members for FMICS'2014.
- W. Serwe was a program committee member for the track on “Prototyping, Validation, Verification, Modeling and Simulation” of VLSI-SOC'2014 (*22nd IFIP/IEEE International Conference on Very Large Scale Integration*), Playa del Carmen, Mexico, October 6–8, 2014.

9.1.2.3. Reviewer

- H. Evrard reviewed articles submitted to FOCLASA'2014 and TACAS'2015 (*21th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*).
- F. Jebali reviewed articles submitted to AVOCs'2014 (*14th International Workshop on Automated Verification of Critical Systems*).
- A. Kriouile reviewed articles submitted to SAC-SVT'2015 (*30th ACM/SIGAPP Symposium on Applied Computing — Software Verification Track*).

- F. Lang reviewed articles submitted to TACAS'2015.
- R. Mateescu reviewed articles submitted to AVOCS'2014, SEFM'2014, and TACAS'2015.
- G. Salaün reviewed articles submitted to WETICE-PASCS'2014 (*23rd IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises — Track on Privacy and Accountability for Software and Cloud Services*).
- W. Serwe reviewed articles submitted to AVOCS'2014, DATE'2014 (*Design, Automation & Test in Europe*), and TACAS'2015.
- L. Ye reviewed articles submitted to SEFM'2014, VALID'2014 (*6th International Conference on Advances in System Testing and Validation Lifecycle*), SAC-SVT'2015, and FSEN'2015 (*6th IPM International Conference on Fundamentals of Software Engineering*).

9.1.3. Journal

9.1.3.1. Member of the editorial board

- H. Garavel is an editorial board member of STTT (*Springer International Journal on Software Tools for Technology Transfer*).
- G. Salaün is an editorial board member of SOCA (*Springer International Journal on Service Oriented Computing and Applications*).

9.1.3.2. Reviewer

- R. Mateescu was reviewer for ACM TECS (*Transactions on Embedded Computing Systems*) and STTT.
- J. I. Requeno was reviewer for IEEE TC (*Transactions on Computers*).
- G. Salaün was reviewer for JLAMP (*Journal of Logical and Algebraic Methods in Programming*), JISA (*Journal of Internet Services and Applications*), IEEE TSE (*Transactions on Software Engineering*), and IJWET (*International Journal of Web Engineering and Technology*).

9.1.4. 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 2014, the main facts are the following:

- We prepared and distributed twelve successive versions (2014-a to 2014-l) of CADP.
- We were requested to grant CADP licenses for 425 different computers in the world.

The CONVECS Web site ⁰ was updated with scientific contents, announcements, publications, etc.

By the end of December 2014, the CADP forum ⁰, opened in 2007 for discussions regarding the CADP toolbox, had over 320 registered users and over 1570 messages had been exchanged.

Also, five large Petri nets derived from our LNT models were provided as benchmark examples for the 2014 edition of the Model Checking Contest.

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:

- The IMCReo tool to reason about QoS in Stochastic Reo connectors [58], [59]
- The Alvis virtual machine to execute formal models in the Alvis language [57]
- The Tomte tool for active learning of Mealy machines [30]
- The Vercors platform for verifying the correct composition of distributed components [52]
- The TLM.open tool connecting SystemC/TLM models to CADP [50]
- The REFINER tool for formal Verification of Model Transformations [65], [66]
- The ELTON development environment for LOTOS specifications [68]

⁰<http://convecs.inria.fr>

⁰<http://cadp.inria.fr/forum.html>

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

- Model-based specification, implementation and testing of a software bus [61]
- Protocol conformance testing using active learning of Mealy machines [31]
- High-performance fractal coherence [64], [63]
- Verification of models reverse engineered from smart-card readers [34]

9.1.5. Awards and Distinctions

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

9.1.6. Lectures and Invited Conferences

- H. Garavel gave an invited talk entitled “Trois décennies de réussite en méthodes formelles” at the Journées MFDL/MTV2 (*Méthodes Formelles pour le Développement de Logiciels/Méthodes de Test pour la Vérification et la Validation*) held on January 14, 2014 in Grenoble, France.
- H. Garavel and R. Mateescu gave a talk entitled “Analyse de traces par model checking / Trace Analysis using Model Checking” at the PIMLIG seminar “Traces dans tous leurs états” held on January 22, 2014 in Grenoble, France.
- G. Salaün gave a talk entitled “On the Verification of Asynchronously Communicating Systems” on February 18, 2014 in Málaga, Spain.
- G. Salaün gave a talk entitled “Verification of Asynchronously Communicating Systems” on October 2nd, 2014 in Clermont-Ferrand, France.
- R. Mateescu gave an invited talk entitled “Walking Back and Forth in Labelled Transition Systems” at the GRAPHITE’2014 workshop held on April 5, 2014, in Grenoble, France.
- H. Garavel gave a talk entitled “Benchmarks and Benchmarking: The Model Checking Contest” at the 20 years of TACAS workshop and celebration held on April 8, 2014 in Grenoble, France.
- H. Garavel gave a talk entitled “Real Time without Clocks” on June 6, 2014 at Saarland University, Saarbrücken, Germany.
- H. Garavel gave a talk entitled “Reconciling Concurrency Theory with Other Branches of Computer Science” at the IFIP WG 1.8 Research Seminar on Open Problems in Concurrency Theory held on June 18–21, 2014 in Bertinoro (Forlì), Italy.
- R. Mateescu gave an invited talk entitled “Mu-Calculus Property-Dependent Reductions for Divergence-Sensitive Branching Bisimilarity” at the WS-FMDS’2014 workshop held on September 2, 2014 in Grenoble, France.
- R. Mateescu gave a talk entitled “Two Decades of Formal Methods for Industrial Critical Systems” at the ERCIM 25th anniversary held on October 23–24, 2014, in Pisa, Italy.
- F. Jebali gave a talk entitled “A Step Towards Reconciling GALS Industrial Design with Formal Verification” on September 11, 2014 at the 11th LASER Summer School on Software Engineering held on September 7–13, 2014 in Elba Island, Italy.
- F. Lang gave a talk entitled “Partial Model Checking Using Labelled Transition Systems and Boolean Equation Systems” to a panel of 1st year students of Ecole Normale Supérieure de Cachan during their visit to the LIG laboratory on December 9, 2014.

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 2014, we carried out the following teaching activities:

- G. Salaün is co-responsible of the ISI (*Ingénierie des Systèmes d'Information*) department of ENSIMAG since September 1, 2011.
- 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 “*Programmation orientée-objet*” to the second year computer science engineering students of ENSIMAG (18 hours).
- G. Salaün gave a course on “*Théorie des langages*” to the first year computer science engineering students of ENSIMAG (18 hours).
- R. Oliveira served as a teaching assistant in a course on “*Bases de Données*”, given by Aurélien Faravelon to the first year computer science engineering students of IUT2 (25 hours).
- R. Oliveira served as a teaching assistant in a course on “*Algorithmique et programmation*”, given by Vanda Luengo to the first year computer science engineering students of IUT (40 hours).

9.2.2. Juries

- G. Salaün was external reviewer for José Antonio Mateo Cortés’s PhD thesis, entitled “*Verification and Validation of Web Service Compositions using Formal Methods*”, defended at Universidad de Castilla La Mancha, Spain, on July 1st, 2014.
- G. Salaün was external reviewer for Diana Allam’s PhD thesis, entitled “*Enforcing Loose Coupling and Substitution Principles in an Object-Oriented Framework for Web Services*”, defended at Ecole des Mines, Nantes, France, on July 10, 2014.
- R. Mateescu was external reviewer for Ala Eddine Ben Salem’s PhD thesis, entitled “*Improving the Model Checking of Stutter-Invariant LTL Properties*”, defended at Université Pierre et Marie Curie, Paris, France, on September 25, 2014.
- G. Salaün was external reviewer for Lakhdar Akroun’s PhD thesis, entitled “*Décidabilité et complexité de la relation de simulation des services Web orientés données*”, defended at Université Blaise Pascal, Clermont-Ferrand, France, on December 8, 2014.
- G. Salaün was external reviewer for Dimitris Vekris’s PhD thesis, entitled “*Vérification de spécifications EB3 à l’aide de techniques de model checking*”, defended at Université Paris-Est Créteil, France, on December 10, 2014.

9.3. Popularization

H. Garavel participates to the committee in charge of organizing the Aerospace Valley series of industrial conferences on formal methods. The third conference ⁰, devoted to theorem proving, held on February 4 in Toulouse and retransmitted by video-conference in Grenoble, attracted over 100 participants from industry and academia.

The fourth conference ⁰, devoted to model checking, held on October 16 in Toulouse and retransmitted by video-conference in Grenoble and Saclay, attracted over 120 participants from industry and academia. H. Garavel gave a talk entitled “*Présentation de l’outil CADP*”. A. Kriouile gave a talk entitled “*Application de CADP à la vérification de matériel*”. R. Mateescu gave a talk entitled “*Introduction au model checking*”.

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.

⁰<http://www.inria.fr/centre/grenoble/agenda/forum-methodes-formelles2>

⁰<http://projects.laas.fr/IFSE/FMF/J4/index.html>

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 Minalogic “*pôle de compétitivité mondial*”.

H. Garavel was a reviewer for various ongoing ANR (*Agence Nationale de la Recherche*) pre-propositions and projects evaluated in 2014.

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*).

G. Salaün is a member of the MSTIC council of Grenoble-Alpes University (*Conseil de pôle MSTIC*).

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

F. Lang is (together with Laurent Lefèvre from the AVALON Inria project-team) correspondent in charge of the Inria Activity Report at Inria Grenoble - Rhône-Alpes.

HYCOMES Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

8.1.1.1. Member of the conference program committee

Benoît Caillaud has served on the program committee of the ACSD 2014 conference

8.1.1.2. Reviewer

Benoît Caillaud has been reviewing for the ACSD 2014, ACC 2014, CONCUR 2014, DATE 2014 and TACAS 2015 conferences.

8.1.2. Journal

8.1.2.1. Reviewer

Benoît Caillaud has been reviewing for the following journals: ACM Transactions on Embedded Computing, Acta Informatica and Emperical Software Engineering.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Benoît Caillaud has taught an invited course on hybrid systems modeling in the first year master curriculum in computer science of ENS Rennes. This was a joint course with Marc Pouzet, representing a total of 27 hours EqTD.

8.2.2. Supervision

PhD in progress : Ayman Aljarbouh, Accelerated simulation of hybrid systems, started December 2013, supervised by Benoît Caillaud

PhD in progress : Guillaume Baudart, Time-based protocols for LTTA, started December 2013, co-supervised by Albert Benveniste and Marc Pouzet (Parkas Inria project-team, ENS, Paris).

MUTANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

8.1.1.1. Chair of conference program committee

Jean-Louis Giavitto was co-chair of the SCW 2014 the Spatial COmputing Workshop, co-located with AAMAS, May 2014, Paris.

8.1.1.2. Member of the conference program committee

Jean-Louis Giavitto has participated in the program committee of the following workshop and conferences: BIPC special track at 8th International Conference on Bio-inspired Information and Communications Technologies - BICT 2014, December, 2014, Boston, MA, USA; MeCBIC 2014 7th Workshop on Membrane Computing and Biologically Inspired Process Calculi, September 2014, Bucharest, Romania; SASO Eighth IEEE International Conference on Self-Adaptive and Self-Organizing Systems - London, September 2014; JIM 2014 Journée d'informatique Musicale - Bourges - mai 2014; Journées nationales du GDR GPL 2014, juin 2014, CNAM Paris.

Florent Jacquemard has participated in the program committee of the 6th International Symposium on Symbolic Computation in Software Science (SCSS 2014) and the conférence Journées d'informatique Musicale (JIM 2014).

8.1.1.3. Reviewer

The members of the team regularly participate as reviewers for IEEE ICASSP, ACM Multimedia Conferences, Sound and Music Computing, International Computer Music Conference (ICMC), Digital Audio Effects Conference (DAFx), European Joint Conferences on Theory and Practice of Software (ETAPS), Federated Logic Conference (FLoC, federating CADE, LICS, RTA), and more.

8.1.2. Journal

8.1.2.1. Member of the editorial board

Jean-Louis Giavitto is the redactor-in-chief of TSI (Technique et Science Informatiques) published by Lavoisier.

8.1.2.2. Reviewer

The members of the team are regular reviewers for IEEE Transactions on topics related to Machine Learning in Signal Processing (IEEE TSALP, TPAMI, Multimedia journals), Theoretical Computer Science related journals (TCS, MFCS, LMCS, JLAP, IPL), and Computer Music related journals (CMJ, JNMR).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Licence : Clement Poncelet, Environnement de développement, 40h, L3, UPMC, France.
- Licence : Clement Poncelet, Ateliers de Recherche Encadrée - ARE, 20h, L1, UPMC, France.
- Licence : José Echeveste, Structures discrètes, 30h, L3, UPMC, France.
- Licence : Arshia Cont, Sound Engineering and New Technologies - Paris Superior Conservatory, 2h/week.

8.2.2. Supervision

- PhD in progress: José Echeveste, Accorder le temps de la machine et celui du musicien, started in october 2011, supervisor: Arshia Cont and Jean-Louis Giavitto.
- PhD in progress: Clément Poncelet, Formal methods for analyzing human-machine interaction in complex timed scenario. Started in october 2013, supervisor: Florent Jacquemard.
- PhD in progress: Philippe Cuvillier, Probabilistic Decoding of strongly-timed events in realtime, supervisor: Arshia Cont.

8.2.3. *Juries*

Jean-Louis Giavitto was reviewer of the Habilitation of Arnaud Banos (Sorbonne – Paris I, Pour des pratiques de modélisation et de simulation libérées en géographie et SHS) and examiners for two PhDs: Mariem Miladi (SupMeca, Modélisation géométrique et mécanique pour les systèmes mécatroniques) et Adrien Basso-Blandin (Université d’Evry, Conception d’un langage dédié à la conception de fonctions biologiques de synthèse par compilation de spécifications comportementales).

Arshia Cont has acted as Reporter for two Habilitation juries in 2014, for Cédric Févotte (University of Nice) on Non-Negative Matrix Factorization and Its Applications, and for Brunno Bossis (University of Rennes 2) on Musicological Tools for analysis of Live Electronic Music.

8.2.4. *Institutional commitment*

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 Verification” pole of the GDR. He is also an expert for the ANR DEFI program and a reviewer for FET projects for the UC.

Florent Jacquemard is member of the IFIP WorkingGroup 1.6 on Term Rewriting.

Arshia Cont is the director of *Research/Creativity Interfaces* at Ircam, in charge of coordinating scientific and artistic activities of the institution and dissemination of its software and community through Ircam Forum.

Arshia Cont is board member of ICMA (International Computer Music Association) since 2014.

8.3. Popularization

Arshia Cont was invited to a **TEDx Talk** in October 2014 on *Human-Computer Musicianship* that attracted more than 12 thousand podcasts according to organisers.

Arshia Cont was invited to participate in CNRS’s 2nd edition of “Les Fondamentales” Science and Society event in Grenoble, in a session dedicated to **Science and Music on the same Score**.

Arshia Cont was invitee to the BFM Business Program on *Future of Sound*.

Arshia Cont was featured in the June Edition of *Usbek et Rica* magazine.

MuTant team participated in the 2014 edition of *Futur en Seine* festival and showcased **collaboration with Orchestre de Paris** in a public event.

Article on Antescofo by Arshia Cont in the December 2014-January 2015 edition of the popular science magazine “Dossier de La Recherche”.

José Echeveste, Arshia Cont and Jean-Louis Giavitto participated to the colloquium “La musique en temps réel” in the festival Musica, Strasbourg, september 2014.

Jean-Louis Giavitto participated to the colloquium “Le calcul et le temps, colloque de philosophie de l’informatique” Université Jean Moulin (Lyon 3), novembre 2014. He was invited on several seminars outside computer sciences: EPFL - ArchiZoom, “computational morphogenesis” in the context of the architecture exhibition “Animal ?” (april 2014); the elmlalfructidor art school in Chalons, “space and the formalization of musical processes” (april 2014); CNSMD Lyon and the Ecole Normale Lyon, “Du temps écrit au temps produit” with Julia Blondeau (april 2014); CISEC (club Inter-associations – AAAF, SEE, SIA – des Systèmes Embarqués Critiques), “Temps Réel en musique : Antescofo” (Toulouse June 2014).

Florent Jacquemard participated to the Inria seminar “1/2 hour of science” in July 2014, with a talk on Testing and Verification of interactive music systems.

PARKAS Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, scientific chair

Albert Cohen was the general chair of PPOPP 2015, and will be the general chair of PLDI 2017 (associated with ECRC).

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

Albert Cohen was the program chair of CC 2014, the TPC chair of the DAC 2014 ESS1 subcommittee, and the program chair of ARCS 2015.

8.1.2.2. Member of the conference program committee

Albert Cohen was a member of the PC of PLDI 2014, of the ERC of PLDI 2015 and PACT 2015, of the ERC of ASPLOS 2014, PPOPP 2014 and ICS 2014.

Marc Pouzet was a member of the PC of DAC (Design Automation Conference) 2014, EOOLT (Equation-Based Object-Oriented Modeling Languages and Tools) 2014, AFADL (Approches Formelles dans l'Assistance au Développement de Logiciels) 2014.

Francesco Zappa Nardelli was a member of the PC of PPOPP (Principles and Practice of Concurrent Programming) 2014 and ESOP (European symposium on programming) 2014.

8.1.3. Journal

8.1.3.1. Member of the editorial board

Albert Cohen is an associate editor of ACM TACO and IJPP (Springer).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

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

Master : M. Pouzet & T. Bourke: "Synchronous Systems" (M2), Lectures and TDs, ENS, France

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

Licence : F. Zappa Nardelli: "Introduction à l'informatique" (L3), TDs, 40h, École Polytechnique, France

Licence : M. Pouzet: "Operating Systems" (L3), Lectures, ENS, France.

Licence : J. Vuillemin & T. Bourke, "Digital Systems", Lectures and TDs, ENS, France

Marc Pouzet is Director of Studies for the CS department, at ENS.

8.2.2. Supervision

HdR : F. Zappa Nardelli, Reasoning between programming languages and architectures, ENS, January 2014

PhD : F. Li, Compiling for a multithreaded dataflow architecture: algorithms, tools, and experience. Université Pierre et Marie Curie - Paris VI, May 2014

PhD in progress : Guillaume Baudart, 2nd year, supervised by T. Bourke and M. Pouzet

PhD in progress : Adrien Guatto, 4th year, supervised by T. Bourke and A. Cohen and M. Pouzet

PhD in progress : Robin Morisset, 2nd year, supervised by F. Zappa Nardelli

M2 Internship : Ulysse Beaugnon (MPRI), supervised by A. Cohen and M. Pouzet.

M2 Internship : Basile Clement (MPRI), supervised by A. Cohen and M. Pouzet.

8.2.3. Juries

- Albert Cohen was a reviewer in the PhD thesis committees of Jarryd Beck (2015, U. New South Wales, Australia), Pranav Tendulkar (2014, U. Grenoble), Cedric Nugteren (2014, T. U. Eindhoven, The Netherlands).
- Albert Cohen was a president in the PhD thesis committees of Sofiane Lagraa (2014, U. Grenoble), Bruno Bodin (2014, UPMC).
- Albert Cohen was examiner in the PhD thesis committee of Victor Lomüller (2014, U. Grenoble).
- Marc Pouzet was president of the Jury for the habilitation of Anne Bouillard, April 8, 2014.
- Marc Pouzet was jury member of the PhD. thesis of Arlen Cox, University of Colorado, Boulder, November 17, 2014.
- Marc Pouzet was member of the committee for the AERES evaluation of the Lab. of SupAero (ISAE), Toulouse, Nov. 2014.
- Marc Pouzet was member of the Prix de thèse du GDR GPL (Génie de la Programmation et du Logiciel).

8.3. Popularization

T. Bourke hosted a tutorial by Makarius Wenzel at ENS Ulm on the Isabelle proof assistant.

SPADES Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. general chair, scientific chair

- Sophie Quinton was PC co-chair and organizing committee member of the *First Workshop on Formal Methods for Timing Verification* (FMTV'14).
- Alain Girault was PC co-chair and co-organizer of the *Second Workshop on Reconciling Performance with Predictability* (RePP'14), which took place on March 5th 2014, in Grenoble, France.
- Alain Girault was co-chair and co-organizer of the *Workshop on Synchronous Programming* (SYNCHRON'14), which took place in December 2014 in Aussois, France.

9.1.2. Scientific events selection

9.1.2.1. Participation in conference steering committees

- Jean-Bernard Stefani is the current chair of the Steering Committee of the *IFIP FORTE* conference series, and a member of the Steering Committee of the *DisCoTec* federated conference series.

9.1.2.2. Participation in conference program committees

- Pascal Fradet served in the program committees of the *13th International Conference on Modularity* (MODULARITY'14) and of *Journées Francophones des Langages Applicatifs* (JFLA'14).
- Gregor Goessler served in the program committees of the *17th International Symposium on Component-Based Software Engineering* (CBSE'14) and *Design, Automation, and Test in Europe* (DATE'14).
- Sophie Quinton served in the program committees of the *26th Euromicro Conference on Real-Time Systems* (ECRTS'14), *34th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems* (FORTE'14) and *12th IEEE International Symposium on Parallel and Distributed Processing with Applications* (ISPA'14) conferences as well as the *First International Workshop on Multi-Objective Many-Core Design* (MOMAC'14) and *2nd International Workshop on Mixed Criticality Systems* (WMC'14) workshops and the Work-in-Progress session of ECRTS'14.
- Alain Girault served on the program committees of the *International Conference on Design and Test in Europe* (DATE'14), the *Design Automation Conference* (DAC'14), the *International Symposium on Industrial Embedded Systems* (SIES'14), and the *International Conference on Pervasive and Embedded Computing and Communication Systems* (PECCS'14).

9.1.2.3. Reviewer

- Gregor Goessler reviewed articles for CDC'14, POST'14, and TACAS'14.
- Sophie Quinton reviewed an article for the *51th Design Automation Conference* (DAC'14).

9.1.3. Journal

9.1.3.1. Member of the editorial board

- Jean-Bernard Stefani is a member of the editorial board of *Annals of Telecommunications*.
- Alain Girault is a member of the editorial board of the *EURASIP Journal on Embedded Systems*.

9.1.3.2. Reviewer

- Jean-Bernard Stefani reviewed articles for *Theoretical Computer Science*.

- Gregor Goessler reviewed articles for *Science of Computer Programming* and *ACM Transactions on Embedded Computing Systems*.
- Sophie Quinton reviewed articles for *ACM Transactions on Embedded Computing*, *ACM Transactions on Design Automation of Electronic Systems* and *Real-Time Systems*.
- Alain Girault reviewed articles for *IEEE Trans. on Parallel and Distributed Systems* and *ACM Trans. on Design Automation of Electronic Systems*

9.2. Teaching - Supervision - Juries

9.2.1. Supervision

PhD in progress: Vagelis Bebelis, “Boolean Parametric Data Flow. Modeling - Analyses - Implementation”, 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, advised by Gregor Goessler.

9.2.2. Juries

- Alain Girault was president of the PhD defense jury of Pranav Tendulkar (University Grenoble Alpes).
- Alain Girault was president of the PhD defense jury of Christian von Essen (University Grenoble Alpes).
- Alain Girault was referee for the computer science PhD thesis of Guillaume Aupy (ENS-Lyon).
- Jean-Bernard Stefani was president of the jury for Bertrand Jeannet’s HDR defense (University Grenoble Alpes).
- Jean-Bernard Stefani was rapporteur for Helene Martorell’s PhD defense (Toulouse University)

TEA Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

Jean-Pierre Talpin is a member of the steering committee of the ACM-IEEE Conference on Methods and Models for System Design (MEMOCODE).

9.1.1.2. responsable of the conference program committee

Jean-Pierre Talpin co-chaired the program committee of the 12th. ACM-IEEE MEMOCODE conference and the 5th. IEEE RTSS workshop AVICPS.

9.1.1.3. member of the conference program committee

Jean-Pierre Talpin served the program committee of the 12th. ACM EMSOFT'14, ACM LCTES'14, and SCOPES'14 conferences, as well as the MODELS workshop ACVI'14.

Thierry Gautier served as program committee member for the 2014 Electronic System Level Synthesis Conference, ESLsyn 2014 (<http://www.ecsi.org/eslsyn>) and for the 12th ACM-IEEE International Conference on Formal Methods and Models for System Design, MEMOCODE'14 (<http://memocode.irisa.fr>).

9.1.2. Journal

9.1.2.1. member of the editorial board

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.

9.1.2.2. reviewer

Jean-Pierre Talpin reviewed for Acta Informatica and Science of Computer Programming.

9.2. Teaching - Supervision - Juries

9.2.1. Supervision

- *PhD advisory of Chan Ngo* by Jean-Pierre Talpin, Paul Le Guernic and Thierry Gautier, entitled "*Vérification formelle d'un générateur de code pour les spécifications polychrones*", defended in December 2014.
- *PhD advisory of Sun Ke* by Jean-Pierre Talpin, Paul Le Guernic and Thierry Gautier, entitled "*Conception conjointe de modules synchrones et de réseaux flot-de-données polychrones*", since 2011.
- *PhD co-advisory of Imré Frotier de la Messelière* by Jean-Pierre Talpin and Pierre Jouvelot (Mines ParisTech), entitled "*Conception et implémentation d'applications musicales innovantes pour les nouvelles technologies multimédia*", since October 2013.

9.2.2. Juries

Jean-Pierre Talpin served as Referee at the Thesis Defence of Vincent Gaudel (UBO), entitled "*Des patrons de conception pour assurer l'analyse d'architectures : un exemple avec l'analyse d'ordonnancement*", December 2014.

ANTIQUÉ Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the steering program committee

Jérôme Feret is member of the Steering Committee of the international Workshop on Static Analysis and Systems Biology (SASB).

9.1.1.2. member of the organizing committee

Tie Cheng was a member of the Organizing Committee of EuSprIG 2014.

Antoine Miné was a member of the Organizing Committee of the 5th Workshop on Tools for Automatic Program Analysis (TAPAS 2014), Munich, Germany, 10 September, 2014.

9.1.2. Scientific events selection

9.1.2.1. responsible of the conference program committee

Xavier Rival was 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, [32]).

9.1.2.2. member of the conference program committee

Jérôme Feret was member 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; of the Program Committee of the Sixth International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2014), CHamonix, France, April 20–24, 2014; of the Program Committee of the 10th International Workshop on Developments in Computational Models (DCM 2014), Vienna, Austria, July 13 2014; of the Program Committee of the International Workshop on Verification of Engineered Molecular Devices and Programs (VEMDP 2014), Vienna, Austria, July 17, 2014; of the Program Committee of the 3rd International Conference on Biomedical Engineering and Biotechnology (iCBEB 2014), Beijing, China, August 18–20, 2014. of the Program Committee of the 8th IFIP International Conference on Theoretical Computer Science (TCS 2014), Rome, Italy, September 1–3, 2014; of the Program Committee of the 5th International Workshop on Static Analysis and Systems Biology (SASB 2014), München, Germany, September 10, 2014; of the Program Committee of the 19th International Workshop on Formal Methods for Industrial Critical Systems (FMICS 2014), Florence, Italy, September 11–12, 2014; Jérôme Feret is member of the Program Committee of of the Program Committee of 11th International Workshop on Developments in Computational Models (DCM 2015), Cali, Colombia, October 28, 2015; of the Program Committee of the 7th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2015), Rome, Italy, May 24–29, 2015; of the Program Committee of the 24th International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR 2015), Siena, Italy, July 13–15, 2015.

Xavier Rival was member of the Program Committee of the 41st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2014 PC), San Diego, USA, January 22-24, 2014; of the Program Committee of the 21st International Static Analysis Symposium (SAS 2014), München, Germany, September 11–13, 2014; of the Extended Review Committee of the 42nd ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2015 ERC), Mumbai, India, January 15-17, 2015.

Antoine Miné was member of the Program Committee of the 5th International Workshop on Polyhedral Compilation Techniques (IMPACT'5), Amsterdam, The Netherlands, the 11th International Conference on Integrated Formal Methods (iFM'14), Bertinoro, Italy, 9–11 September 2014, the 11th School on MODelling and VERifying parallel Processes (MOVEP'14), Nantes, France, 7–11 July 2014, and the 8th International Symposium on Theoretical Aspects of Software Engineering (TASE'14), Changsha, China, 1–3 September 2014. Antoine Miné was member of the External Review Committee of the 42nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'14), Mumbai, India, 11-18 January 2015. Antoine Miné is member of the Program Committee of the 22nd International Static Analysis Symposium (SAS'15), Saint-Malo, France, 9–11 September 2015, and the 9th International Symposium on Theoretical Aspects of Software Engineering (TASE'15), Nanjing, China, 12–14 September 2015.

Caterina Urban is member of the Competition Jury for the 4th Competition on Software Verification (SV-COMP 2015) to be held at TACAS 2015 in London, UK.

9.1.2.3. reviewer

Arlen Cox was a reviewer for the 21st International Static Analysis Symposium (SAS 2014), München, Germany, September 11–13, 2014.

Jérôme Feret was a reviewer for the 42nd ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2015), Mumbai, India, January 15–17, 2015, and for the 18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2015), London, UK, April 11–18, 2015.

Xavier Rival was a reviewer for the Symposium on Programming Languages Design and Implementation (PLDI 2014), Edimburgh, UK, June 9–11, 2014, and for the AVICPS Workshop, Rome, Italy, December 2, 2014.

Antoine Miné was a reviewer for the 12th Asian Symposium on Programming Languages and Systems (APLAS 2014), Singapore, November 17-19, 2014, the 35th annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI 2015), Edinburgh, UK, 9–11 June 2014, and the 21st International Static Analysis Symposium (SAS 2014), Munich, Germany, September 11–13, 2014.

Caterina Urban was reviewer for the conference Theoretical Computer Science (TCS), Roma, Italy, 1–3 September 2014, and the 26th International Conference on Computer Aided Verification (CAV 2014), Vienna, Austria, 18–22 July, 2014.

9.1.3. Journal

9.1.3.1. member of the editorial board

Jérôme Feret is a member of the editorial board of the [Frontiers in Genetics](#) journal and the [Open Journal of Modelling and Simulation](#)

Antoine Miné is member of the editorial board of The Scientific World Journal and of Conference Papers in Computer Science.

9.1.3.2. reviewer

In 2014, Jérôme Feret was a reviewer for BMC Systems Biology; Software, Practice and Experience; Transactions on Modeling and Computer Simulation; PLOS Computational Biology; BMC Bioinformatics; and Axioms.

Antoine Miné was a reviewr for the Computer Languages, Systems & Structures journal, the Software and Systems Modeling journal, and the Transactions on Programming Languages and Systems journal.

9.1.4. Grants selection

9.1.4.1. reviewer

Jérôme Feret was a reviewer for the Swiss National Science Foundation.

9.1.5. Participation in Conferences

- CAV: Arlen Cox and Caterina Urban attended the conference on Computer Aided Verification (Vienna, Austria, July 22, 2014). Arlen Cox gave a talk on “QUICr: A Parametric Abstraction Domain for Sets of Numbers”.
- ECCB: Wassim Abou-Jaoudé attended the European Conference on Computational Biology (Strasbourg, France, September, 2014) and gave an invited talk on [8] at the workshop on Logical Modelling and Analysis of Cellular Networks.
- ESOP: Antoine Miné and Caterina Urban attended the 23rd European Symposium on Programming (Grenoble, France); Caterina Urban presented an article [27].
- EuSprIG: Tie Cheng attended the Conference of the European Spreadsheet Risk Interest Group (EuSprIG, July 2014).
- ISOLA: Xavier Rival attended the International Symposium On Leveraging Applications of Formal Methods, Verification and Validation (Corfu, Greece, October 2014), and presented an article [24].
- ITP: Arnaud Spiwack attended the International Conference on Interactive Theorem Proving (ITP 2014, Vienna, July 2014), and presented an article [23].
- JRSIF: Mehdi Bouaziz attended the research day of SIF “De la formation à l’innovation en Informatique”, (Paris, France, September 2014).
- JSTools: Arlen Cox attended the workshop on JavaScript Tools (Uppsala, Sweden, July 28, 2014) and gave a talk on “JSAna with HOO: Automatically Verifying JavaScript Libraries without Client Code”.
- LICS: Patrick Cousot, Jérôme Feret, and Caterina Urban attended the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2014, Vienna, July 2014). Patrick Cousot gave an invited talk on [10].
- LSB: Jérôme Feret attended the 5th Workshop on Logic and Systems Biology (LSB 2014, Vienna, July 2014) and gave an invited talk on [16].
- NSAD: Mehdi Bouaziz, Tie Cheng, Arlen Cox, Antoine Miné, Xavier Rival, Antoine Toubhans and Caterina Urban attended the Workshop on Numerical and Symbolic Abstract Domains (NSAD 2014, München, Germany, September 2014).
- OCaml meetup: Mehdi Bouaziz attended the OCaml meetups (Paris, France, September and December 2014). Thibault Suzanne attended an OCaml meetup and gave a talk on “Implémentation d’une structure de données : Hash Array Mapped Tries”.
- POPL: Mehdi Bouaziz, Patrick Cousot, Radhia Cousot, Arlen Cox, Jérôme Feret, Antoine Miné, Xavier Rival and Caterina Urban attended the Symposium on Principles Of Programming Languages (POPL 2014, San Diego, USA); Xavier Rival chaired a session; Caterina Urban presented a poster.
- SAS: Mehdi Bouaziz, Tie Cheng, Patrick Cousot, Arlen Cox, Jérôme Feret, Antoine Miné, Xavier Rival, Antoine Toubhans, Caterina Urban, and Thibault Suzanne attended the Static Analysis Symposium (SAS 2014, München, Germany, September 2014); Xavier Rival chaired a session; Arlen Cox presented an article [14]; Antoine Toubhans presented an article [25]; Caterina Urban presented an article [26].
- SASB: Wassim Abou-Jaoudé and Jérôme Feret attended the Workshop on Static Analysis and Systems Biology (SASB 2014, München, Germany, September 2014). Jérôme Feret presented an article [16].
- TAPAS: Mehdi Bouaziz, Tie Cheng, Patrick Cousot, Arlen Cox, Antoine Miné, Xavier Rival, Antoine Toubhans and Caterina Urban attended the Workshop on Tools for Automatic Program Analysis (TAPAS 2014, München, Germany, September 2014).
- TYPES: Mehdi Bouaziz attended the Types 2014 meeting (TYPES 2014), Paris, France, May 2014).

VEMDP: Jérôme Feret attended the International Workshop on Verification of Engineered Molecular Devices and Programs (VEMDP 2014, Vienna, Austria, July 2014).

VMCAI: Mehdi Bouaziz, Patrick Cousot, Radhia Cousot, Arlen Cox, Jérôme Feret, Antoine Miné, Xavier Rival and Caterina Urban attended the Conference on Verification, Model-Checking and Abstract Interpretation (VMCAI 2014, San Diego, USA); Xavier Rival chaired the conference [32]; Jérôme Feret chaired a session; Antoine Miné presented an article [21].

WODES: Wassim Abou-Jaoudé attended the International Workshop on Discrete Event Systems (WODES 2014, Cachan, France, May 2014).

WST: Caterina Urban attended the 14th International Workshop on Termination and presented an article [30].

9.1.6. Seminars and talks

- Wassim Abou-Jaoudé gave some talks on “Logical modeling of T-helper cell differentiation and plasticity” [8] at Instituto Gulbenkian de Ciência (Oeiras, Portugal) in June 2014 and Max Planck Institute for Molecular Genetics (Berlin, Germany) in November 2014.
- Mehdi Bouaziz attended to the Dagstuhl Seminar on Next Generation Static Analysis Tools (Wadern, Germany) in August 2014 and gave two talks on “Introduction to Abstract Interpretation: static analysis and beyond” at the séminaire des doctorants du département d’informatique de l’École normale supérieure (ENS Paris, Paris, France) in November 2014, and at the Séminaire Francilien de Sûreté de Fonctionnement, (École Centrale Paris) in November 2014.
- Arlen Cox gave a talk on “HOO: Heap with Open Objects” at the Dagstuhl Seminar for Scripting Languages and Frameworks: Analysis and Verification (Wadem, Germany) in June 2014, a talk on “Statically Analyzing Object-Manipulating JavaScript Libraries without Client Code” at the Institute for Defense Analysis (Bowie, Maryland, USA) in September 2014, and talks on “JSAna with HOO: Automatically Verifying JavaScript Libraries without Client Code” at Facebook (London, U.K) in August 2014, at Cyberpoint Lab (Baltimore, Maryland, USA) in September 2014, at Apple (Cupertino, California, USA) in November 2014, at Draper Labs (Boston, Massachusetts, USA) in November 2014, and at MathWorks (Natick, Massachusetts, USA) in November 2014.
- Jérôme Feret gave a talk “An algebraic approach for inferring and using symmetries in rule-based models” at the Dagstuhl Seminar on Next Generation Static Analysis Tools (Wadern, Germany) in August 2014 and a talk on “Rule-Based Modeling” at the Dagstuhl Seminar on Multiscale Spatial Computational Systems Biology (Wadern, Germany) in November 2014
- Xavier Rival gave a talk “Towards precise and scalable static analyses” at the 54th IFIP WG 2.4 Group Meeting (Monterey, California, USA) in February 2014, a talk on “Verification of safety critical embedded software” at the Retraite du Département d’Informatique (Belleme, Normandie, France) in May 2014, talks on “Modular Construction of Shape-Numeric Analyzers” at Aarhus University (Aarhus, Denmark) in June 2014, at East China Normal University (Shanghai, China) in July 2014 and at Northern University for Defense Technology (Changsha, China) in July 2014, a talk on “Construction of abstract domains for heterogeneous memory properties” at the Dagstuhl Seminar on Next Generation Static Analysis Tools (Wadern, Germany) in August 2014, and a talk on “Type Verification of Spreadsheet Applications” at the 55th IFIP WG 2.4 Group Meeting (Stellenbosch, South Africa) in November 2014.
- Antoine Toubhans gave a talk on “Composite abstract domains for shape analysis” at the Seminar of the Gallium Group (Inria Paris-Rocquencourt), in September 2014.
- Antoine Miné gave a talk on “ A method to infer inductive numeric invariants inspired from Constraint Programming” at Decision Procedures and Abstract Interpretation (Dagstugh Seminar 14351) in August 2014, a seminar on “Mixing abstract interpretation and constraint programming techniques” at Laboratoire VERIMAG (Grenoble, France) in October 2014, a poster presentation on “The Astrée static analyzer” at Evaluating Software Verification Systems: Benchmarks and Competitions (Dagstugh Seminar 14171) in April 2014.

- Caterina Urban gave a seminar on “Proving Guarantee and Recurrence Temporal Properties by Abstract Interpretation” at University of Udine (Italy) in December 2014, a seminar on “Proving Guarantee and Recurrence Temporal Properties by Abstract Interpretation” at ETH Zurich in November 2014, a seminar “Automatic Inference of Ranking Functions by Abstract Interpretation” at Queen Mary University of London in October 2014, a talk on “Automatic Inference of Ranking Functions by Abstract Interpretation” at Dagstuhl Seminar 14352 “Next Generation Static Software Analysis Tools” in August 2014, a seminar on “Automatic Inference of Ranking Functions by Abstract Interpretation” at University College London in June 2014, a seminar on “An Abstract Domain to Infer Ordinal-Valued Ranking Functions” at Inria Rennes, Rennes in May 2014, a seminar on “Automatic Inference of Ranking Functions by Abstract Interpretation” at Séminaire du DI ENS in May 2014, a seminar on “Automatic Inference of Ranking Functions by Abstract Interpretation” at Inria Paris-Rocquencourt in March 2014, a seminar on “Automatic Inference of Ranking Functions by Abstract Interpretation” at IBM Thomas J. Watson Research Center in January 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence:
 - Mehdi Bouaziz, Concepts Informatique (CI2), 22 ETD, L1, Université Paris-Diderot, Paris, France.
 - Mehdi Bouaziz, Intensive training in algorithmics, 35 ETD, Epita, Le Kremlin-Bicêtre, octobre-novembre 2014.
 - Mehdi Bouaziz, Preparation to the International Olympiad in Informatics, 40h ETD, Epita, Le Kremlin-Bicêtre, France.
 - Tie Cheng, Introduction to algorithmics, 36h ETD, L3, École Polytechnique, Palaiseau, France.
 - Jérôme Feret, and Caterina Urban, Mathematics, 40h ETD, L1, FDV Bachelor program (Frontiers in Life Sciences (FdV)), Université Paris-Descartes, France.
 - Antoine Miné and Xavier Rival, Semantics and applications to verification, 48h ETD, L3, École Normale Supérieure, Paris, France.
 - Xavier Rival, Introduction to static analysis, 8h, L3, École des Mines de Paris, Paris, France.
 - Xavier Rival, Introduction to algorithmics, 40h ETD, L3, École Polytechnique, Palaiseau, France.
 - Antoine Toubhans, Functional Analysis Class, 34h ETD, L2, Université Pierre et Marie Curie (UPMC), Paris, France.
 - Caterina Urban, Mathematics, 26.5h ETD, Bachelor Program “Frontières du Vivant”, Université Paris Descartes.
 - Thibault Suzanne, Introduction to Programming, 72h ETD, L1, Université Paris Diderot.
- Master:
 - Vincent Danos and Jérôme Feret (with Jean Krivine), Computational Biology, 20h 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, Introduction to abstract interpretation, 8h, M1-M2, East China Normal University, Shanghai, China.

9.2.2. Supervision

PhD:

- Arlen Cox, Parametric heap abstraction for dynamic languages libraries, University of Colorado at Boulder (USA), 17 of November 2014, supervised jointly by Bor-Yuh Evan Chang (University of Colorado), Xavier Rival (École Normale Supérieure) and Sriram Sankaranarayana (University of Colorado).

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, supervised jointly by Bor-Yuh Evan Chang (University of Colorado), Xavier Rival (École Normale Supérieure) and Sriram Sankaranarayana (University of Colorado).
- 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.
- Huisong Li, Static Analysis of Data-Structures with Sharing, November 2014, Xavier Rival, 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.
- Thibault Suzanne, Thread-modular static analysis of concurrent programs in the presence of weak memory models, October 2014, Antoine Miné, École Normale Supérieure.

9.2.3. Juries

Jérôme Feret was in the jury of the PhD thesis of Arlen Cox (17 of November 2014, University of Colorado, Boulder, USA). Jérôme Feret was reviewer of the PhD thesis of Peter Kreyßig (to be defended, Friedrich Schiller University, Jena, Germany).

Xavier Rival took part to the jury of the Habilitation Thesis of Francesco Zappa-Nardelli (16th of January 2014, ENS Paris) and to the jury of the Habilitation Thesis of Bertrand Jeannet (27 of March 2014, Université Joseph Fourier, Grenoble).

Antoine Miné is reviewer for the PhD thesis of Vivien Maisonneuve (École des Mines de Paris, February 2015). Antoine Miné was reviewer and in the jury of the PhD thesis of Julien Henry (Université de Grenoble, 13 October 2014).

9.3. Popularization

Mehdi Bouaziz gave a course on “Apprendre et enseignement — la programmation informatique des bibliothèques”, Maire de Paris, 12 hours, june-july 2014. Xavier Rival gave a talk on “Safety critical embedded softwares and their verification” at the Ceremony for the “Médailles of Engineering Sciences” in April 2014. Xavier Rival participated to the organization of the “Nuit des Sciences” in June 2014.

CELTIQUE Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific events organisation

7.1.1.1. general chair, scientific chair

- EJCP 2014 (École jeunes chercheurs en programmation): Thomas Jensen, Alan Schmitt.

7.1.1.2. member of the organizing committee

- PLMW 2014 (Programming Languages Mentoring Workshop): Alan Schmitt.

7.1.2. Scientific events selection

7.1.2.1. responsible of the conference program committee

- GraMSec 2014 (International Workshop on Graphical Models for Security): Barbara Kordy.

7.1.2.2. member of the conference program committee

- ESOP 2014 (European Symposium on Programming): David Pichardie.
- ITP 2014 (Interactive Theorem Proving): David Pichardie.
- CC 2014 (Compiler Construction): Sandrine Blazy
- VSTTE 2014 (Verified Software: Theories, Tools and Experiments): Sandrine Blazy
- AFADL 2014 (Approches Formelles dans l'Assistance au Développement de Logiciels) : Sandrine Blazy
- WASMAS (Active Security Through Multi-Agent Systems): Barbara Kordy.

7.1.2.3. reviewer

- ESOP 2014 (European Symposium on Programming): Delphine Demange, Alan Schmitt, Thomas Jensen.
- FLOPS 2014 (Symposium on Functional and Logic Programming): Alan Schmitt.
- ICFP 2014 (International Conference on Functional Programming): Alan Schmitt.
- IFIP SEC 2014 (International Information Security and Privacy Conference): Frédéric Besson, Thomas Jensen.
- ITP 2014 (Interactive Theorem Proving): Delphine Demange.
- LICS 2014 (Logic In Computer Science): Delphine Demange.
- POPL 2014 (Symposium on Principles of Programming Languages): David Pichardie
- PPDP 2014 (Principles and Practice of Declarative Programming): Alan Schmitt.
- PEPM 2015 (Partial Evaluation and Program Manipulation): Thomas Jensen.
- CC 2014 (Compiler Construction): Sandrine Blazy
- VSTTE 2014 (Verified Software: Theories, Tools and Experiments): Sandrine Blazy
- AFADL 2014 (Approches Formelles dans l'Assistance au Développement de Logiciels) : Sandrine Blazy
- POST 2014 (Conference on Principles of Security and Trust): Barbara Kordy.
- TACAS 2014 (International Conference on Tools and Algorithms for the Construction and Analysis of Systems): Barbara Kordy.
- GraMSec 2014 (International Workshop on Graphical Models for Security): Barbara Kordy.

- WASMAS 2014 (Active Security Through Multi-Agent Systems): Barbara Kordy.
- FORTE 2014 (International Conference on Formal Techniques for Distributed Objects, Components and Systems): Barbara Kordy.
- PRDC 2014 (IEEE Pacific Rim International Symposium on Dependable Computing): Barbara Kordy.
- STM 2014 (International Workshop on Security and Trust Management): Barbara Kordy

7.1.3. Journal

7.1.3.1. reviewer

- Logical Methods in Computer Science: Alan Schmitt.
- Science of Computer Programming: Alan Schmitt.
- Journal of Computer Security: Sandrine Blazy
- Journal of Formalized Reasoning: Frédéric Besson, Sandrine Blazy.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence: Delphine Demange, Functional Programming, 70h, L1, Université de Rennes 1 / Istic, France

Licence: Thomas Genet, Software Engineering, 58h, L2, Université de Rennes 1 / Istic, France

Licence: Delphine Demange, Software Engineering, 40h, L2, Université de Rennes 1 / Istic, France

Licence : Sandrine Blazy, Functional programming in OCaml, 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, 36h, L3, ENS Rennes, France

Licence : David Cachera, Logic, 36h, L3, ENS Rennes, France

Licence : David Pichardie, Algorithms, 36h, L3, ENS Rennes, France

Licence : Alan Schmitt, Programmation Fonctionnelle, 37h, L3, Insa Rennes, France

Licence : Barbara Kordy, Formal Languages and Grammars, 36h , L3, INSA Rennes, France

Master : Thomas Genet, Formal Design and Verification, 108h, M1, Université de Rennes 1 / Istic, France

Master : Thomas Genet, Cryptographic Protocols, 24h, M2, Université de Rennes 1 / Istic, France

Master : Frédéric Besson, Compilation, 68h, M1, Insa Rennes, France

Master : Alan Schmitt, Méthodes Formelles pour le développement de logiciels sûrs, 22h, M1, Rennes 1, France

Master : David Cachera, Semantics of Programming Languages, 36h, M1, Université Rennes 1, France

Master : Delphine Demange, Software Security, 9h, M2, Université Rennes 1, France

Master : David Pichardie, Software Security, 21h, M2, Université Rennes 1, France

Master : David Pichardie, Mechanized Semantics, 15h, M2, Université Rennes 1, France

Master : Thomas Jensen, Static Analysis and Software Security, 20h, University of Copenhagen, Denmark.

Master : Barbara Kordy, Security, 17h, M2, INSA Rennes, France

Master : Barbara Kordy, 4th year Project, 55h, M1, INSA Rennes, France

7.2.2. *Supervision*

PhD in progress : Martin Bodin, Certified Analyses of JavaScript, 1st september 2012, Thomas Jensen and Alan Schmitt

PhD in progress : Vincent Laporte, Formal verification of static analyses for low level langages, 1st septembre 2012, Sandrine Blazy and David Pichardie

PhD in progress : Yannick Zakowski, Programs Logics for Concurrency, 1st september 2014, David Pichardie and David Cachera

PhD in progress: Pierre Wilke, Low-level memory models for compilers and static analysers, 1st august 1013, Sandrine Blazy and Frédéric Besson

PhD in progress: Yann Salmon, Reachability for Term Rewriting Systems under Strategies, from Sept 2012, Thomas Genet

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: Stéphanie Riaud, Transformations de programmes pertinentes pour la sécurité du logiciel, septembre 2011, Sandrine Blazy

PhD: Valérie Murat, Tree Automata Extensions for the Verification of Infinite State Systems, Université de Rennes 1, Thomas Genet

PhD: Andre Oliveira Maroneze, Verified Compilation and Worst-Case Execution Time Estimation, Université de Rennes 1, Sandrine Blazy, David Pichardie and Isabelle Puaut

7.2.3. *Juries*

Thomas Genet, jury member (reviewer) for the PhD defense of Marc Sylvestre, October 2014, University Bordeaux 1

Alan Schmitt, jury member for the PhD defense of Alain Mebsout, September 2014, Laboratoire de Recherche en Informatique

Alan Schmitt, jury member (reviewer) for the PhD defense of Nuno Gaspar, December 2014, Université de Sophia-Antipolis

Thomas Jensen, jury member (reviewer) for the PhD defense of Jael Kriener, March 2014, University of Kent at Canterbury, UK

David Pichardie, jury member (chair) for the PhD defense of Sebastien Chedor, January 2014, University Rennes 1, France

David Pichardie, jury member (examiner) for the PhD defense of Jonathan Protzenko, September 2014, University Paris-Diderot, France

David Pichardie, jury member (chair) for the PhD defense of Hernan Vanzetto, December 2014, University of Lorraine, France

David Pichardie, jury member (chair) for the PhD defense of Radoniaina Andriatsimandefitra Ratsisahanana, December 2014, SUPELEC, France

Sandrine Blazy, jury member (reviewer) for the PhD defense of Vincent Benayoun, May 2014, CNAM, France

Sandrine Blazy, jury member (chair) for the PhD defense of Van Chan Ngo, July 2014, University Rennes 1, France

Sandrine Blazy, jury member (reviewer) for the PhD defense of Etienne Millon, July 2014, University Paris 6, France

Barbara Kordy, jury member, (reviewer) for the PhD defense of Hannes Holm, February 2014, KTH, Sweden.

7.2.4. Juries for competitive selections

Sandrine Blazy, jury member and external president for the selection of a Maître de Conférences, May 2014, University Paris Sud, France.

Sandrine Blazy, jury member for the selection of a Maître de Conférences, May 2014, INSA de Rennes, France.

Sandrine Blazy, jury member for the selection of a Professeur des Universités, May 2014, University Paris Diderot, France.

Sandrine Blazy, jury member for the final selection of Inria DR (senior researchers) candidates, June 2014, Inria, Paris, France.

Sandrine Blazy, member of the evaluation committee CES 28 of ANR for the competitive selection of ANR projects, June 2014, Paris, France.

Delphine Demange, jury member for the selection of a Maître de Conférences at University of Rennes 1 / ISTIC, May 2014, University of Rennes 1, France.

Delphine Demange, jury member of the Gilles Kahn PhD award committee, December 2014, Inria Paris - Rocquencourt, Antenne Parisienne, France.

7.3. Popularization

- Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, for high school teachers, ENS Rennes, Oct. 2014.

DEDUCTEAM Exploratory Action

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, scientific chair

Catherine Dubois was a general chair of the GDR GPL national days, and the AFADL'14, CAL'14, and CIEL'14 conferences, organized at *Cnam* in Paris.

8.1.1.2. Member of the organizing committee

David Delahaye was a member of the organizing committee of the GDR GPL national days, and the AFADL'14, CAL'14, and CIEL'14 conferences, organized at *Cnam* in Paris.

Olivier Hermant and Florian Rabe organized the 2nd KWARC-Deducteam workshop in Bremen, Germany (May 2014).

Gilles Dowek is a member of the steering committees of RTA and TLCA. Catherine Dubois is the chair of the steering committee of TAP.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

Gilles Dowek has been the PC chair of RTA-TLCA.

David Delahaye and Catherine Dubois were co-chairs of the SETS'14 workshop (affiliated to ABZ'14).

David Delahaye was a co-chair of the $\forall X.XII$ '14 workshop (affiliated to VSL'14).

Catherine Dubois was a co-chair of the F-IDE'14 workshop (affiliated to ETAPS'14). She was also a PC co-chair of the AFADL'2014 national conference.

8.1.2.2. Member of the conference program committee

Olivier Hermant was member of the program committee of the RTA-TLCA 2014 conference (July 2014).

8.1.2.3. Reviewer

Frédéric Blanqui reviewed a paper submitted to the post-proceedings of TYPES'14.

Alejandro Díaz-Caro reviewed a paper submitted to the FSTTCS'14 conference.

Ronan Saillard reviewed a paper submitted to the RTA'14 conference.

8.1.3. Journal

8.1.3.1. Member of the editorial board

David Delahaye is a member of the editorial board of the Global Journal of Advanced Software Engineering (GJASE).

8.1.3.2. Reviewer

David Delahaye reviewed one paper for the Global Journal of Advanced Software Engineering (GJASE) and one paper for the Requirements Engineering (RE) journal.

Alejandro Díaz-Caro reviewed a paper submitted to Elsevier's "Science of Computer Programming" journal.

Olivier Hermant reviewed a paper submitted to the journal "Theoretical Computer Science".

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

CPGE: Simon Cruanes, Mathématiques-Informatiques en MPSI, 64 HETD, MPSI, Lycée Saint-Louis, France.

Licence : Raphaël Cauderlier, Eléments de programmation 2, 63 HETD, L1, UPMC, France.

Licence: Ali Assaf, Algorithmique et programmation, 36 HETD, L3, Ecole Polytechnique, France.

Licence: Ali Assaf, Les bases de la programmation et de l'algorithmique, 36 HETD, L3, Ecole Polytechnique, France.

Licence : Alejandro Díaz-Caro, Mathématiques 2, 18 HETD, L1, Université Paris-Ouest Nanterre La Défense, France.

Licence : Alejandro Díaz-Caro, Méthodologie de la mesure en sciences humaines, 48 HETD, L1, Université Paris-Ouest Nanterre La Défense, France.

Licence : Alejandro Díaz-Caro, Statistiques et probabilités, 18 HETD, L2, Université Paris-Ouest Nanterre La Défense, France.

Licence : Alejandro Díaz-Caro, Probabilités, 36 HETD, L2, Université Paris-Ouest Nanterre La Défense, France.

Licence : Alejandro Díaz-Caro, Probabilités, 36 HETD, L2, Université Paris-Ouest Nanterre La Défense, France.

Licence: Ronan Saillard, Programmation Orientée Objet en Java, 27 HETD, Telecom ParisTech, France.

Licence: Guillaume Burel, Programmation avancée, 25.5 HETD, L3, ENSIIE, France

Licence: Guillaume Burel, Logique, 10.5 HETD, L3, ENSIIE, France

Licence: Guillaume Burel, Projet informatique, 22.75 HETD, L3, ENSIIE, France

Master: Guillaume Burel, Systèmes et langages formels, 17.5 HETD, M1, ENSIIE, France

Master: Guillaume Burel, Compilation, 33.25 HETD, M1, ENSIIE, France

Licence: Guillaume Burel is in charge of the 4th, 5th, and 6th semesters of the engineering degree at ENSIIE.

Licence: Pierre Halmagrand, Initiation à la Programmation en JAVA, 48.75 HETD, L1, CNAM, France

Master: Pierre Halmagrand, Initiation à la Méthode B, 53.7 HETD, M2, CNAM, France

Master: Gilles Dowek has given invited classes at Supelec, Centrale, INSA-Lyon.

8.2.2. Supervision

PhD : Kim-Quyen Ly, Automated verification of termination certificates [11], University Joseph Fourier, Grenoble, 9 October 2014, Jean-François Monin and Frédéric Blanqui.

PhD in progress : Ronan Saillard, Systèmes de Types Modulo, Oct 2012, Olivier Hermant and Pierre Jouvelot.

PhD in progress : Pierre Halmagrand, “Automated Deduction Modulo”, from Oct. 2013, David Delahaye, Olivier Hermant, and Damien Doligez.

PhD in progress : Guillaume Bury, “SMT Modulo”, Oct. 2014, David Delahaye.

PhD in progress : Ali Assaf, Interoperability of Proof Systems, Oct. 2012, Gilles Dowek and Guillaume Burel.

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, October 2012, Gilles Dowek.

8.2.3. Juries

David Delahaye reviewed the PhD thesis of Hernán Vanzetto, supervised by Stephan Merz and Kaustuv Chaudhuri, and defended in Dec. 2014 in Nancy.

David Delahaye was part of the HDR jury of Stéphane Lengrand, defended in Dec. 2014 at École Polytechnique in Palaiseau.

Gilles Dowek has been part of the HDR committee of Philippe Malbos.

Catherine Dubois reviewed the HDR thesis of Oum-El-Kheir Aktouf, defended in July 2014 in Valence.

8.3. Popularization

Gilles Dowek is the president of the scientific board of the “Société Informatique de France” (SIF).

Gilles Dowek is a member of the scientific board of “La Main à la Pâte”.

Raphaël Cauderlier, Simon Cruanes, Pierre Halmagrand et Ronan Saillard ont participé à l’animation du stand Inria au Salon Culture et Jeux Mathématiques les 24 et 25 mai

Ali Asaf, Raphaël Cauderlier, Simon Cruanes et Pierre Halmagrand ont participé à l’animation du stand Inria lors de la Fête de la Science les 9 et 10 octobre 2014 à Paris

Gilles Dowek has given a talk at Mathenjeans.

Alejandro Díaz-Caro is member of the scientific board of “Ensemble”, a journal of the Maison Argentina at Cité Universitaire in Paris, ISSN 1852–5911.

ESTASYS Exploratory Action

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, Scientific chair

- Axel Legay has been tutorial chair for the *European Joint Conferences on Theory and Practice of Software (ETAPS)*

8.1.1.2. Member of the organizing committee

- Axel Legay was a member of the organization committee for the *European Joint Conferences on Theory and Practice of Software (ETAPS)*

8.1.2. Scientific events selection

8.1.2.1. Responsible of the conference program committee

- Axel Legay has been the Program Chair for *Formal Modelling and Analysis of Timed Systems* conference
- Axel Legay has been the Program Chair for *From Programs to Systems – The Systems Perspective in Computing* workshop organized in honour of Joseph Sifakis
- Axel Legay has been the Program Chair for *Software Product Line Analysis Tools* workshop

8.1.2.2. Member of the conference program committee

- Axel Legay was PC member of MEMOCODE, FORMATS, FORMALIZE, SPLC, ASE, FACS, FORTE.
- Louis-Marie Traonouez was PC member of FORMATS
- Rudolf Fahrenberg was PC member of MFCS

8.1.3. Journal

8.1.3.1. Member of the editorial board

- Axel Legay is a member of the editorial board of the newly created journal for masterminding changes (FOMACS).

8.1.4. Teaching

Software Verification

Axel Legay: Software Verification, 40 hours, Royal Holloway, University of London

Axel Legay: Modélisation et Vérification Formelle par Automates, 12 hours, University of Rennes 1.

Rudolf Fahrenberg: Modélisation et Vérification Formelle par Automates, TP 12 hours, University of Rennes 1.

Louis-Marie Traonouez: Verification et Test des Systemes Embarques, 20 hours, ESIR Rennes.

8.1.5. Supervision

PhD : Cyrille Jegourel, Rare event techniques for Statistical Model checking, Novembre 2011, Axel Legay

8.1.6. Juries

Axel Legay has been a member of the PhD jury for Hoa Lee (Trento), Maxime Cordy (Namur), and Cyrille Jegourel (Rennes).

GALLIUM Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Maxime Dénès was member of the organizing committee for the First International Workshop on Coq for Programming Languages (**CoqPL 2015**), co-located with POPL'15 in Mumbai, India.

9.1.2. Scientific events selection

9.1.2.1. Chair of the conference program committee

Xavier Leroy co-chaired the program committee of the ACM SIGPLAN 2015 conference on Certified Proofs and Programs (**CPP'15**), which will take place in January 2015 in Mumbai, India, colocated with POPL'15.

9.1.2.2. Member of the conference program committee

- **ALENEX 2015** (Algorithm Engineering & Experiments): Umut Acar was a member of the program committee.
- **ECOOP 2014** (European Conference on Object-Oriented Programming): Mike Rainey was a member of the artefact evaluation committee.
- **ESOP 2015** (European Symposium on Programming): Umut Acar was a member of the program committee.
- **Eurosys 2015** (European Conference on Systems Research and Development): Pierre-Évariste Dagand was a member of the shadow program committee.
- **POPL 2015** (42nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages): Umut Acar and François Pottier were members of the program committee; Xavier Leroy was a member of the external review committee.
- **CoqPL 2015** (Workshop on Coq for Programming Languages): Maxime Dénès and Xavier Leroy were members of the program committee.
- **MLW 2015** (ACM SIGPLAN ML Family Workshop): Didier Rémy was a member of the program committee.
- **WGP 2014** (Workshop on Generic Programming): Pierre-Évariste Dagand was a member of the program committee.

9.1.2.3. Reviewer

In 2014, members of Gallium reviewed approximately 95 papers submitted to international conferences and 15 papers submitted to international workshops.

9.1.3. Journals

9.1.3.1. Member of the editorial board

- **Communications of the ACM**: Xavier Leroy is on the editorial board for the Research Highlights column.
- **Journal of Automated Reasoning**: Xavier Leroy is a member of the editorial board.
- **Journal of Functional Programming**: François Pottier is a member of the editorial board.
- **Journal of Formalized Reasoning**: Xavier Leroy is a member of the editorial board.

9.1.3.2. Reviewer

In 2014, members of Gallium reviewed 4 journal submissions.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Umut Acar and Mike Rainey, “Introduction to parallel computing with PAsL”, 15h, L2, University of Puerto Rico, USA.

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, “IP1: Introduction to computer science and programming using Java”, 42h, L1, University Paris Diderot, France.

Licence: Gabriel Scherer, “IP1: Introduction to computer science and programming using C”, 42h, L3, University Paris Diderot, France.

Master: Xavier Leroy and Didier Rémy, “Functional programming languages”, 15h + 20h, M2R MPRI, University Paris Diderot/ENS Paris/ENS Cachan/Polytechnique, France.

Master: Luc Maranget, “Semantics, languages and algorithms for multi-core programming”, 9h, M2 MPRI, University Paris Diderot/ENS Paris/ENS Cachan/Polytechnique, France.

Master: François Pottier, “Compilation” (INF564), 13h30, M1, École Polytechnique, France.

9.2.2. Supervision

PhD: Çağdas Bozman, “Profilage mémoire d’applications OCaml”, Ecole Polytechnique, defended on 16 Dec 2014, supervised by Michel Mauny (ENSTA), Pierre Chambart (OCamlPro), and Fabrice Le Fessant (Inria).

PhD: Julien Cretin, “Erasable coercions: a unified approach to type systems” [11], École Polytechnique, defended on 30 Jan 2014, supervised by Didier Rémy.

PhD: Jonathan Protzenko, “Mezzo: a typed language for safe effectful concurrent programs” [12], U. Paris Diderot, defended on 29 Sep 2014, supervised by François Pottier.

PhD in progress: Arthur Guillon, “Concurrent realizability and program verification for weak memory computers”, U. Paris Diderot, started September 2014, interrupted January 2015, supervised by Luc Maranget and Jade Alglave (Microsoft Research Cambridge).

PhD in progress: Pierre Halmagrand, “Dédution Automatique Modulo”, CNAM, since September 2013, supervised by David Delahaye (CNAM), Damien Doligez (Inria), and Olivier Hermant (Mines ParisTech).

PhD in progress: Gabriel Scherer, “Term inference: proof search for singleton inhabitants”, 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.

Pre-PhD ENS year: Thomas Williams, “Putting ornaments into practice”, since September 2014, supervised by Didier Rémy.

9.2.3. Juries

Damien Doligez was a member of the Ph.D. jury of Çağdas Bozman, ENSTA ParisTech, Palaiseau, December 2014.

Xavier Leroy chaired the PhD committee of André Maroneze, University Rennes 1, June 2014.

Xavier Leroy was a member of the committees for the PhD awards of ACM SIGPLAN and of the GDR GPL (*Génie de la Programmation et du Logiciel*).

9.2.4. Collective responsibilities

Damien Doligez chaired the *Commission des actions de développement technologiques* of Inria Paris-Rocquencourt until Oct 2014.

Xavier Leroy is *vice-président du comité des projets* of Inria Paris-Rocquencourt and appointed member of Inria's *Commission d'Évaluation*. He participated in the following Inria hiring and promotion committees: *jury d'admissibilité CR2 Saclay*; *jury d'admissibilité DR2*; *promotions CR1*; *promotions DR1 and DR0*.

Luc Maranget is an elected member of the *Comité Technique Inria*.

Luc Maranget chairs the *Commission des utilisateurs des moyens informatiques – Recherche* of Inria Paris-Rocquencourt.

Didier Rémy is deputy scientific director of Inria, in charge of the fields Algorithmics, Programming, Software and Architecture.

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.

9.3. Popularization

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

Jacques-Henri Jourdan manned a stand at “Salon Culture & Jeux Mathématiques”, in Paris.

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 2014, with 23 posts from 5 different authors.

MARELLE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events selection

9.1.1.1. Member of the conference program committee

Benjamin Grégoire was member of the program committee for the conference TCS (Theoretical Computer Science), which was held on September 1-3 in Roma, Italy.

Yves Bertot was member of the programm committee for the conference ITP (Interactive Theorem Proving), which was held July 14-17 in Vienna, Austria and for the workshop UITP (User Interfaces for Theorem Provers), which was on held on July 17th in Vienna, Austria.

Laurent Théry was member of the programm committee for the conferences ITP (Interactive Theorem Proving) and UITP (User Interfaces for Theorem Provers) in Vienna (see above) and for the workshop ACL2 (International Workshop on the ACL2 Theorem Prover and its Applications), which was held July 12-13 in Vienna, Austria.

9.1.1.2. Reviewer

Members of the team reviewed papers for the conferences CPP (Certified Programs and Proofs), CCS (ACM Conference on Computer and Communication Security), CSF (Computer Security Foundations), Types (Types for Proofs and Programs),.

9.1.2. Journal

9.1.2.1. Member of the editorial board

Laurent Théry was a special issue editor for Mathematics in Computer Science, "Special Focus on Formal Proofs for Mathematics and Computer Science".

9.1.2.2. Reviewer

Members of the team reviewed papers for the journals JFP (Journal of Functional Programming), TOPLAS (Transactions on Programming Languages and Systems), MSCS (Mathematical Structures in Computer Science), JFR (Journal of Formalized Reasoning), TCS (Journal of Theoretical Computer Science), AMAI (Annals of Mathematics and Artificial Intelligence), and SCP (Science of Computer Programming).

9.1.2.3. Evaluation of funded grants

Laurence Rideau evaluated a grant proposal for the Digiteo laboratory (based in Saclay).

Yves Bertot evaluated a grant proposal for the European Research Concil (consolidator grants).

Laurent Théry evaluated a grant proposal for the French Research Agency (ANR).

9.2. Participation in scientific events

9.2.1. Keynotes, tutorials, and invited talks

Yves Bertot gave an invited talk at the conference CICM (Conference on Intelligent Computer Mathematics) in Coimbra, Portugal, in July.

Laurent Théry, Laurence Rideau, and Yves Bertot gave invited talks at the workshop "Mathematical Structures of Computation", special week on "Formal Proof, Symbolic Computation and Computer Arithmetic", in Lyon, France, in February.

Yves Bertot gave talks at the University of Edinburgh in June, at the NASA Ames research center in California, in June, at SRI in California, in June, at the University of Aveiro in July, and at the University of Tokyo in September. He also attended the ACM Award ceremony in San Francisco, California, in June.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Licence : Laurence Rideau, "programming and algorithms", 50 hours, Lycée Masséna, Nice, France.

Master : Yves Bertot, "software verification and computer proof", 21 hours, Master, Université de Nice, France.

Master : Laurent Théry, "introduction to Coq", 3 hours, Ecole des Mines de Paris, France.

Doctorate : Yves Bertot, Formal proofs in coq, 10 hours, NII Shonan, Japan

Doctorate : Benjamin Grégoire, Proofs in Easycrypt, 9 hours, Inria, France

9.3.2. Supervision

PhD : Guillaume Cano, "Intéraction entre algèbre linéaire et analyse en mathématiques formelles", Université de Nice, 4 avril 2014, supervised by Yves Bertot [19].

9.3.3. Juries

Yves Bertot was examiner with written report duty for the thesis of Pierre Boutillier (Université de Paris-Diderot, France, February 18th), external examiner for the thesis of Phil Scott (university of Edinburgh, Scotland, June 4th), and examiner with written report duty for the Habilitation of Sylvie Boldo (Université de Paris-Sud, France, October 6th).

Laurent Théry was examiner for the thesis of Anders Mörtberg (Chalmers University, Sweden, December 12th), This thesis was partially supervised by Cyril Cohen.

9.3.4. 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 commission on continued training and a commission on hygiene, safety, and working conditions. This activity involves around 12 meetings per year.
- Benjamin Grégoire is a member of the *committee of users of information technology* (CUMI). This activity involves monthly meetings where problems in using the IT infrastructure are debated between researchers and engineers.
- Laurent Théry is a member of the *comité de développement technologique* (in English, technological development committee), the committee that oversees the allocation of software engineers on experimental software and platform development.
- Laurent Théry is a member of the committee that provides advice to the center director concerning the attribution of grants for doctoral students, post-doctoral researchers, and invited professors.
- Yves Bertot is the chairman of the *Coq Steering committee*. Benjamin Grégoire was a member of this committee until October and has been replaced by *Enrico Tassi*. These tasks imply continuous monitoring of the evolution of Coq, the relations with users, and participating in strategic decisions.
- Yves Bertot was deputy scientific director for the Sophia Antipolis méditerranée research center until August. This task implies meetings approximately every fortnight with the center director, the scientific director, and the director of administrative 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. Yves Bertot still participates to the evaluation committee at national level.

9.4. Popularization

Laurent Théry presented his researcher work to three different classrooms during the event "semaine des maths", in March.

MEXICO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, Scientific chair

- Serge Haddad was co-chair for workshop and tutorials for 34th Int. Conf. on Application and Theory of Petri nets (ATPN), Tunis, Tunisia

9.1.1.2. Member of the organizing committee

- Paul Gastin co-organized the Dagstuhl seminar on "Quantitative Models: Expressiveness, Analysis, and new applications", January 19 to 24, see <http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=14041>.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committee

- Serge Haddad was a member of the program committees of
 - FOR-MOVES (associated with ICSOC 2014),
 - 22nd International Conference on Real Time Networks and Systems (RTNS 2014), Versailles, France,
 - 8th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2014), Bejaia, Algeria,
 - PNSE 2014,
 - 12th IFAC - IEEE International Workshop on Discrete Event Systems (WODES), Cachan, France
- Stefan Haar was a member of the program committees of PNSE 2014 and ETFA 2014. He will be co-chairing the PC of ACSD 2015 (Brussels) and be a member of the PC for ICTAC 2015.
- Thomas Chatain was a member of the program committee of ACSD 2014 and will be a member of the PC of ACSD 2015.
- Stefan Schwoon was a member of the PC of ICATPN 2014 and will be in the PCs for ICATPN 2015 and SPIN 2015.
- Benedikt Bollig was a member of the scientific committee of the workshop INFINITY' 14, co-located with FSTTCS' 14.

9.1.2.2. Reviewer

- Benedikt Bollig was a reviewer for AFL' 14, DLT' 14, TACAS' 14, FOSSACS' 14, ICALP' 14, CSL-LICS' 14, CONCUR' 14, MFCS' 14, TIME' 14, FSTTCS' 14.
- Stefan Haar was a reviewer for CDC 2014 and ACC 2015.
- Stefan Schwoon was a reviewer for the conferences POST, CSL-LICS, and ICALP in 2014.

9.1.3. Journal

9.1.3.1. Member of the editorial board

- Paul Gastin is on the advisory boards of *Journal of Automata, Languages and Combinatorics* and of the EATCS Springer Book series *Monographs in Theoretical Computer Science* and *Texts in Theoretical Computer Science*.

- Serge Haddad was Editor of one edition of the TOPNOC journal (LNCS 8910).
- Stefan Haar is an associate editor for the *Journal of Discrete Event Dynamic systems*.

9.1.3.2. Reviewer

- Benedikt Bollig was a reviewer for *ACM Transactions on Computational Logic, Theoretical Computer Science*, and *Acta Informatica*.
- Stefan Haar was a reviewer for *Automatica, Journal of Computer and System Sciences, IEEE Transactions on Automatic Control*, and *Information Systems*
- Thomas Chatain was a reviewer for *International Journal of Foundations of Computer Science* and *ACM Transactions on Embedded Computing Systems*.
- Stefan Schwoon acted as reviewer for the journals *Fundamenta Informaticae* (several occasions), *TOPLAS*, and *TECS* in 2014.
- Paul Gastin and Serge Haddad are regularly reviewers for many international conferences and journals.

Serge Haddad was also a member of the AERES evaluation committee of the VERIMAG laboratory in 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Note: We only list here the teaching activities of researchers, not the courses of full-time teachers in the team.

Master

Benedikt Bollig and Paul Gastin, Non-Sequential Theory of Distributed Systems, 24 heures de cours, M2, ENS de Cachan

9.2.2. Supervision

PhD :

- Benoît Barbot, *Acceleration for Statistical Model Checking* [11]; ENS Cachan, Defence on November 20, 2014. Supervisor : Serge Haddad and Claudine Picaronny.
- Aiswarya Cyriac, *Verification of Communicating Recursive Programs via Split-width* [12], ENS Cachan, Defence on January 28, 2014; Supervisors: Paul Gastin and Benedikt Bollig
- Hernán Ponce de León, *Testing Concurrent Systems Through Event Structures* [13], ENS Cachan, Defence on November 7, 2014; Supervisor: Stefan Haar, Co-supervisor: Delphine Longuet (U Paris SUD)

PhD in progress :

- Simon Theissing, *Supervision for Multi-Modal Transport Systems*, since September 2013, Supervisor Stefan Haar
- Salim Perchy (Ecole Polytechnique), *D-spaces*, since November 2013, Supervisor Stefan Haar, Co-Supervisor Franck Valencia (Note : S. Perchy belongs to the COMETE team, not MEXICO).

9.2.3. Juries

- Paul Gastin was the president of the PhD examination board of Vincent Carnino, U. Paris-Est, december 5, 2014.
- Stefan Haar was a reviewer of the theses of Sébastien CHEDOR at University of Rennes 1 and of Kari KÄHKÖNEN at Aalto University, Finland.
- Serge Haddad was a reviewer of the thesis of Ariane Piel defended in October 2014 at U. Paris-Nord (Villetaneuse), and of the thesis of Mouhamadou Tafsir Sakho at U. Orléans in December 2014. He also was a member of the PhD juries of Thomas Husja (UPMC, october 2014).
- Stefan Schwoon was a reviewer for the theses of Stanislav Böhm (University of Ostrava, Czechia) and Ala Eddine Ben Salem (Université Paris 6).

9.3. Popularization

- Stefan Haar gave a talk entitled "Revèle tes défauts" on fault diagnosis in the popularization series "Unithé ou café" of Inria Saclay-Idf, on February 7, 2014.

PARSIFAL Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, scientific chair

K. Chaudhuri and L. Straßburger co-chaired the 3rd International Workshop on Structures and Deduction (SD), which was associated with the Federated Logic Colloquium (FLoC) and part of the Vienna Summer of Logic (VSL 2014), Vienna, Austria.

D. Miller was a PC chair for the Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic (CSL14) and the 29th ACM/IEEE Symposium on Logic in Computer Science (LICS14), 14-18 July, Vienna.

8.1.1.2. Member of the organizing committee

K. Chaudhuri was Publicity co-chair for CSL-LICS 2014.

8.1.2. Scientific events selection

8.1.2.1. Member of the conference program committee

K. Chaudhuri was on the Program Committees of:

30th International Conference on Logic Programming (ICLP)

4th ACM-SIGPLAN Conference on Certified Programs and Proofs (CPP)

9th International Workshop on Logical Frameworks and Meta-languages: Theory and Practice (LFMTP)

3rd International Workshop on Linearity

D. Ilik was on the Program Committee of the 16th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014), Canterbury, United Kingdom.

D. Miller was on the Program Committee of WoLLIC 2014: Workshop on Logic, Language, Information and Computation, Valparaiso Chile, 1-4 September.

L. Straßburger was the Program Committee of the 18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS).

8.1.2.2. Reviewer

S. Graham-Lengrand was a reviewer for the following conferences:

International Joint Conference on Automated Reasoning (IJCAR 2014)

Conferences on Intelligent Computer Mathematics (CICM 2014).

L. Straßburger was reviewer for the following conferences:

7th International Joint Conference on Automated Reasoning (IJCAR 2014)

41st International Colloquium on Automata, Languages and Programming (ICALP 2014)

Joint meeting of the 23rd EACSL Annual Conference on Computer Science Logic and the 29th Annual ACM/IEEE Symposium on Logic in Computer Science (CSL-LICS 2014)

F. Lamarche was a reviewer for the following conferences:

Joint International Conferences, Rewriting Techniques and Applications, Typed Lambda Calculus and Applications (RTA - TLCA 2014)

18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS).

D. Ilik was a reviewer for the following conferences:

16th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014), Canterbury, United Kingdom

18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2015)

20th Conference "Types for Proofs and Programs" (TYPES 2014)

24th European Symposium on Programming (ESOP 2015)

Joint International Conferences, Rewriting Techniques and Applications, Typed Lambda Calculus and Applications (RTA - TLCA 2014)

8.1.3. Journal

8.1.3.1. Editor-in-chief

D. Miller was Editor-in-Chief of the ACM Transactions on Computational Logic.

8.1.3.2. Member of the editorial board

S. Graham-Lengrand was guest editor for the special issue on computational logic in honour of Roy Dyckhoff, in the *Journal of Logic and Computation* (2014) [29]

D. Miller is on the editorial board of the following journals: *ACM Transactions on Computational Logic*, *Journal of Automated Reasoning* (Springer), *Theory and Practice of Logic Programming* (Cambridge University Press), and *Journal of Applied Logic* (Elsevier).

8.1.3.3. reviewer

S. Graham-Lengrand was a reviewer for the following journals:

Logic Journal of the IGPL (OUP)

Information and Computation (Elsevier)

Acta Informatica (Springer)

Theoretical Computer Science (Elsevier).

L. Straßburger was reviewer for the following journals:

Archive for Mathematical Logic (Springer)

ACM Transactions on Computational Logic (ACM-ToCL)

F. Lamarche was reviewer for the following journal:

Annals of Pure and Applied Logic (Elsevier).

D. Ilik was reviewer for the following journals:

Logic Journal of the IGPL (OUP)

Mathematical Reviews (MathSciNet)

Theoretical Computer Science (Elsevier)

Zentralblatt MATH

D. Miller was reviewer for the *Studia Logica* journal.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: K. Chaudhuri, “INF 321 : Les principes des langages de programmation”, 40 hours eq. TD, L3, Ecole polytechnique, France

Licence: S. Graham-Lengrand, “*INF431: Algorithmique et programmation*”, 50 hours eq. TD, L3, Ecole Polytechnique, France.

Licence: S. Graham-Lengrand, “*INF412: Les bases de la programmation et de l’algorithmique*”, 32 hours eq. TD, L3, Ecole Polytechnique, France.

Master: S. Graham-Lengrand, “*INF551: Computer-aided reasoning*”, 36 hours eq. TD, M1, Ecole Polytechnique, France.

Master: S. Graham-Lengrand, “*Curry-howard correspondence for classical logic*”, 12 hours eq. TD, M2, Master Parisien de Recherche en Informatique, France.

Master: D. Miller, “*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*”, 12 hours, M2, Master Parisien de Recherche en Informatique, France.

8.2.2. Supervision

PhD: Hernán Vanzetto, “*Automatisation des preuves et synthèse des types pour la théorie des ensembles dans le contexte de TLA⁺*”, Université de Lorraine, 4 Dec 2014; supervised by Stephan Merz (Inria Lorraine) and K. Chaudhuri

PhD in progress: Sonia Marin, 1 Nov 2014, supervised by L. Straßburger and D. Miller

PhD in progress: Roberto Blanco, Zakaria Chihani, and Quentin Heath, supervised by D. Miller

8.2.3. Juries

L. Straßburger was external reviewer and jury member for the PhD of Roman Krenický, University of Manchester, UK. Defence date: April 28, 2014.

S. Graham-Lengrand was a jury member for the PhD of Luis Pino Duque, École Polytechnique, France. Defence date: September 25, 2014.

D. Miller was a reporter for the following two PhD theses: Taus Brock-Nannestad (IT University of Copenhagen, 12 September 2014) and Thanos Tsouanas (ENS Lyon, 2 July 2014).

PI.R2 Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Collective responsibilities

Pierre-Louis Curien was a member of the Conseil Scientifique of the INSII (CNRS), until September 2014. 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.

Frédéric Loulergue is a member of the editorial board of Scalable Computing: Practice and Experience, and Technique et Science Informatiques.

Hugo Herbelin, Pierre Letouzey and Matthieu Sozeau are co-editors of the post-proceedings of the conference TYPES 2014 which was held in Paris in May.

7.1.3. Program committees and organising committees

Alexis Saurin has been a PC member of GaLoP 2014 (International Workshop on Games and Logic for Programming) which took place during ETAPS 2014 in Grenoble, as well as FSTTCS 2014, which took place in Mumbai in December. He is in the PC of WoC 2015, the workshop on continuations, affiliated with ETAPS.

Alexis Saurin is member of the Education committee of the ACM Special Interest Group on Logic (SIGLOG, <http://siglog.hosting.acm.org>).

Hugo Herbelin, Pierre Letouzey and Matthieu Sozeau co-organised and co-chaired the TYPES'14 conference in Paris in May.

Yves Guiraud and Philippe Malbos were among the organisers of the 5-week programme Mathematical Structures of Computation, held in Lyon in January-February 2014, and supported by the Labex MILYON. They were 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.

Yves Guiraud is in the organising committee and PC co-chair of Higher-Dimensional Rewriting and Applications (HDRA), a workshop of the International Conference on Rewriting, Deduction and Programming (RDP) 2015.

Pierre-Louis Curien, Hugo Herbelin and Paul-André Melliès were the organisers of the IHP trimester Semantics of proofs and certified mathematics (cf. highlights). They also organised a spring school at CIRM preceding the trimester, in April 2014.

Pierre-Louis Curien and Hugo Herbelin are members of the steering committee of the conference Typed Lambda Calculi and Applications (TLCA).

Pierre-Louis Curien is a member of the steering committee of the international workshop Games for Logic and Programming Languages (GaLop).

Frédéric Loulergue is a member of the steering committee of the international symposium on High-Level Parallel Programming and Applications (HLPP), he is a member of the program committee of the International Conference on Computational Science (ICCS'15).

Yann Régis-Gianas, Pierre Letouzey, Matthieu Sozeau are the organisers of the “Ecole de Printemps d’Informatique Théorique 2015” about proof of programs. This school has been accepted as a “Ecole Théorique” of the CNRS.

Matthieu Sozeau is a member of the steering committee of the Dependently Typed Programming international workshop (DTP).

Matthieu Sozeau co-organised and chaired the first Coq for Programming Languages (CoqPL) workshop, collocated with POPL'15 in Mumbai, India, in January 2015.

7.1.4. Jury participation

Alexis Saurin has been a member of the Jury for LMFI Master.

Yann Régis-Gianas has been a member of the “Comité de Sélection” for an assistant professor position at the University of Paris Sud.

Pierre-Louis Curien has been a member of the “Comité de Sélection” for a professor position in computer science at the University Paris Diderot.

Matthieu Sozeau has been a member of the Student Research Competition Jury at ICFP 2014 in Gothenburg.

7.1.5. Invited talks

P.-L. Curien gave an invited talk at the workshop “Algebra and Computation” in Lyon (mentioned above).

J.-J. Lévy wrote a paper for P.-L. Curien’s Festschrift Volume, entitled “On the length of Standard Reductions in the Lambda Calculus” [2] (corresponding to his talk back in September 2013 in Venice at the anniversary meeting in his honour).

P.-L. Curien and J.-J. Lévy participated to Luca Cardelli’s Festschrift at Microsoft Research in Cambridge, UK (September 8-9). They gave talks entitled “Around formal parametricity” and “Simple Proofs for Simple Programs”, respectively.

J.-J. Lévy participated to Matthew Hennessy’s Festschrift at IMD in Lucca, Italy (October 15-16). He gave a talk on “Simple Proofs for Simple Programs”.

J.-J. Lévy and A. Saurin participated to “Les Journées LAC (Logique, Algèbre, Calcul)” in Chambéry, France (November 20-21). They gave talks on “Simple Proofs for Simple Programs” and “On the dependencies of logical rules”, respectively.

J.-J. Lévy participated to “The 2nd Locali workshop” between Institute of Software, Chinese Academy of Sciences and Inria/Paris 7 (November 24-26). He gave a talk on “Simple Proofs for Simple Programs”.

M. Sozeau gave an invited talk on “Universe Polymorphism: Subtyping and unification” at the XIXth Agda meeting in Paris (May 2014).

L. Patey has been invited to give a talk at the Workshop on Computability Theory 2014, at a special session of the conference Computability in Europe 2015 and to a Dagstuhl Seminar 2015.

7.1.6. Presentation of papers

Philippe Malbos has presented [31] at IWC 2014.

Marc Lasson has presented [24] at MFPS 2014.

Hugo Herbelin has presented his joint work with Danko Ilik on the computational content of Gödel’s completeness theorem at the workshop PSC 2014.

Matthieu Sozeau has presented [27] at ITP 2014 and [28] at UNIF 2014.

Ludovic Patey received the best student paper award for his paper about dichotomy theorems and an extended version of his paper submitted to the Computability journal has been accepted.

7.1.7. Other presentations

Yann Régis-Gianas gave a talk about Coq at the PPS-LIAFA “pedagogical” meeting.

Frédéric Loulergue gave a short talk at JFLA’15 and a talk at the International Symposium on Symbolic and Numeric Algorithms for Scientific Computing SYNASC’14 (Timisoara).

Matthieu Sozeau gave talks on the development of Coq at the Coq Workshop in Vienna (July 2014) and at the CoqPL workshop in Mumbai (Jan 2015). He also gave a talk on generalised rewriting strategies at TYPES 2014 and at the Coq Workshop.

7.1.8. Talks in seminars

Lourdes González gave a talk on “Incrémentalité dans le calcul” during the Journées PPS, September 2014.

Marc Lasson gave talks about parametricity for dependent types at the TYPES 2014 workshop, at the journées nationales du GDR IM 2014, and the following team seminars: séminaire LCR, LIPN, Paris 13; séminaire Logique et Interactions, Institut de Mathématiques de Marseille; séminaire d’équipe ACADIE, IRIT Toulouse. He also presented his plugin during a Coq working group held in Paris.

Eric Finster gave a talk on Homotopy Type Theory at the “Notions of Identification” seminar at L’équipe ERC Philosophy of Canonical Quantum Gravity, Paris 7 and a talk entitled “Opetopic Diagrams as a Language for Higher Categorical Proofs” at the IHP Trimester in Paris.

Alexis Saurin gave a talk in PARSIFAL seminar at LIX on dependency and correctness of proof-nets.

Matthieu Sozeau gave a talk at the Deducteam seminar at Inria (place d’Italie) on the formalisation of the groupoid model of type theory.

Pierre-Louis Curien gave a seminar talk at the University of Talca (Chile) on “Revisiting the categorical interpretation of type theory” (March).

7.1.9. Attendance to conferences, workshops, schools,...

Lourdes González attended TYPES 2014 in Paris and the IHP trimester “Semantics of proofs and certified mathematics”.

Marc Lasson attended TYPES 2014 in Paris, the IHP trimester, and the Homotopy Type Theory Workshop held at the Mathematical Institute, University of Oxford, in November 2014.

Frédéric Loulergue attended SYNASC 2014 in September (Timisoara), and the JFLA’15 in Val d’Ajol.

Eric Finster attended the IHP Trimester in Paris, and the Homotopy Type Theory Workshop at Oxford.

Alexis Saurin and Matthieu Sozeau attended JFLA 2014, the IHP trimester, Types 2014 and FLOC 2014.

Matthieu Sozeau attended the Heidelberg Laureate Forum in September 2014 and ICFP’14.

7.1.10. Groupe de travail *Théorie des types et réalisabilité*

This is one of the working groups of PPS, jointly organised by Hugo Herbelin and Paul-André Mellès, since September 2009. It is held weekly. Matthieu Sozeau joined the organisation this year.

Internal speakers this year were Eric Finster on Higher Dimensional Syntax and Ludovic Patey on an Introduction to reverse mathematics. The external speakers were Jean-Baptiste Jeannin (CMU), Matthias Puech (McGill University), Sylvain Schmitz (ENS Cachan), Timothy Bourke (Inria and ENS), Cătălin Hrițcu (Inria), Pierre-Evariste Dagand (Inria), Carsten Schürmann (ITU Copenhagen), Conor McBride (Strathclyde University), Nicolas Pouillard (IT University of Copenhagen, Denmark), Alois Brunel (LIPN).

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence: Lourdes González has a temporary research and teaching position (A.T.E.R) at University Paris 7 for the academic year 2014–2015. During the first semester (Sep-Dec 2014) she was in charge of TP (Travaux pratiques, 24 hours) on the subject “Principes de fonctionnement des machines binaires” (L1).

Licence: Étienne Miquey was in charge of TP (Travaux pratiques, 24 hours) in the course “Introduction à la programmation” (L1) at University Paris 7 during the first semester 2014/15.

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).

Master: Alexis Saurin taught, jointly with Christine Tasson, a Master 2 course in “Logique Mathématique et Fondements de l’Informatique” (LMFI), Université Paris Diderot, entitled “Lambda-calcul: des abstractions aux applications”. He taught about 30H. In addition, Saurin chairs LMFI M2 from september 2013.

Master: Yann Régis-Gianas took part in the MPRI course entitled “Type systems”: he taught 12 hours about generalised algebraic data types, higher-order Hoare logic and dependently typed programming.

MOOC: In collaboration with Roberto Di Cosmo and Ralf Treinen, Yann Régis-Gianas wrote a proposal for a MOOC about the OCaml programming language. The proposal has been accepted and the course is in preparation.

Master: Matthieu Sozeau teaches in the MPRI course on Advanced uses of Proof Assistants (12 hours + a project), together with Assia Mahboubi (Inria SpecFun).

Master: Matthieu Sozeau taught an introductory course on software verification to M2 Pro students at University Paris 7 during the first semester (Lectures + Practical Works, 20h).

7.2.2. Supervision

Internship: Alexis Saurin has supervised the L3 internship of Paul Fermé.

Internship: Alexis Saurin has supervised the M1 internship of Simon Lunel.

Internship: Alexis Saurin has supervised, with David Baelde, the M2 internship of Amina Doumane.

Internship: Yann Régis-Gianas has supervised the M2 internship of Thibaut Girka.

Internship: Yann Régis-Gianas has supervised the M2 internship of Thomas Refis.

Internship: Yann Régis-Gianas has supervised the M1 internship of Grégoire Duchêne.

Internship: Yann Régis-Gianas has supervised the M1 internship of Alexandre Ly.

Internship: Matthieu Sozeau has supervised the M2 internship of Philipp Haselwarter.

PhD in progress: Lourdes del Carmen González Huesca, Un langage de tactiques typées pour Coq, December 2011, supervised by Hugo Herbelin and Yann Régis-Gianas.

PhD in progress: Guillaume Claret, Programmation avec effets en Coq, September 2012, supervised Hugo Herbelin and Yann Régis-Gianas.

PhD in progress: Pierre-Marie Pédro, Logique linéaire et types dépendants, september 2012, supervised by Alexis Saurin and Hugo Herbelin.

PhD in progress: Thibaut Girka, Sémantique différentielle, October 2014, supervised by Roberto DiCosmo and Yann Régis-Gianas.

PhD in progress: Cyrille Chenavier, Méthodes algébriques pour la réécriture linéaire, supervised by Yves Guiraud and Philippe Malbos.

PhD in progress: Maxime Lucas, Résolutions polygraphiques cubiques et théorie de Garside, supervised by Yves Guiraud and Pierre-Louis Curien.

PhD in progress: Jovana Obradović, Langages pour la description de différentes sortes d’opérades, supervised by Pierre-Louis Curien.

PhD in progress: Amina Doumane, Ludique, automates, points fixes, supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien.

PhD in progress: Étienne Miquey, Réalisabilité classique et effets de bords, September 2014, supervised by Hugo Herbelin and Alexandre Miquel.

7.2.3. *Juries*

Pierre-Louis Curien was president of the thesis juries of Aloïs Brunel (Univ. Paris 13), Guillaume Jaber (Univ. Nantes), Valentin Blot (ENS Lyon), and Marc Bagnol (Univ. Marseille).

Pierre-Louis Curien was president of the habilitation jury of Philippe Malbos (Univ. Lyon 1).

He is a referee for the habilitation theses of Olivier Serre (LIAFA), Russ Harmer (ENS Lyon), and Paul-André Melliès.

Frédéric Loulergue was president of the thesis juries of Hélène Coullon (Univ. Orléans), Mouhamadou Sakho (Univ. Orléans) and Nader Khammassi (ENSTA Bretagne) ; referee for the theses of Nuno Gaspar (Univ. Nice), Nader Khammassi (ENSTA Bretagne) and Charif Mahmoudi (Univ. Paris-Est Créteil) ; supervisor of the thesis of Thomas Pinsard (Univ. Orléans).

7.3. Popularization

Pierre-Louis Curien wrote the editorial of a special “hors série” issue of the information letter of The Fondation Sciences Mathématiques, entitled “Des preuves et des programmes”, may 2014. He wrote an introductory article “Formalisation mathématique, certification logicielle, même combat!” in the journal *Gazette des Mathématiciens* 142, 83-86 (octobre 2014).

Lourdes González-Huesca and Étienne Miquey took part in the animation of the “Fête de la Science” event at the University Paris 7.

Étienne Miquey took part in the animation of several activities about mathematics in elementary and high schools of Paris.

Yann Régis-Gianas co-organised the “Journée Francilienne de Programmation”, a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS).

Yann Régis-Gianas organised the “Fête de la Science” event for the computer science department of the University Paris 7.

Yann Régis-Gianas and Pierre Letouzey took part in the “Salon Culture et Jeux mathématiques” at Saint Sulpice, Paris.

Yann Régis-Gianas gave several conferences about “What is programming?” in elementary and high schools of Paris.

SUMO Project-Team

9. Dissemination

9.1. Administrative duties

Éric Badouel is secretary of the Permanent Committee of CARI, co-Director of LIRIMA, and the Scientific Manager for Africa and Middle-East region at Inria DRI.

Nathalie Bertrand is secretary and committee member of Gilles Kahn PhD prize.

Éric Fabre is the co-director of the joint research lab of Alcatel-Lucent Bell Labs France and Inria, together with Olivier Audouin on Bell Labs' side. This lab has currently five active joint research teams. Éric Fabre is also member of the Scientific Committee of the joint lab of Alstom and Inria.

Blaise Genest is member of the *Comité de Centre* of Inria Rennes, and of the CNRS CRFP of Bretagne.

Loïc Héliouët was member of the hiring committee a associate professor at INSA Rennes. Loïc Héliouët is currently *réfèrent chercheur* (advisor) for Inria Rennes sharing this responsibility with Christine Morin.

Thierry Jérón is member of the IFIP Working Group 10.2 on Embedded Systems. He is vice-chairman of the project committee of Inria Rennes - Bretagne Atlantique. He gave an invited lecture on "Model-based conformance test generation for timed systems" at WODES'2014. He was member of 3 committees to hire Inria junior scientists (CR2 at Lille and Saclay and CR1)

9.2. Promoting Scientific Activities

9.2.1. Scientific events organisation

9.2.1.1. general chair, scientific chair

Nathalie Bertrand is an elected steering committee member for the international conference QEST (Quantitative Evaluation of Systems).

Thierry Jérón was member of the steering committee of Movep 2014 in Nantes (July 2014).

Hervé Marchand is 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).

9.2.2. Scientific events selection

9.2.2.1. chair/member of conference program committee

Éric Badouel has served in the Programme Committee of BPM'2014 Demos and CARI'2014.

Nathalie Bertrand was PC co-chair of QAPL'14 with L. Bortolussi. She was on the program committee of workshops PRUV'14 and QAPL'14, and of the international conferences QEST'14, TACAS'14.

Loïc Héliouët was member of the program committee of SAM'2014.

Thierry Jérón was PC member of ICTSS 2014, PECCS 2014, SAC-SVT 2014, TAP 2014, WODES 2014, and the forthcoming TAP 2015.

Hervé Marchand was PC member of the WODES conference and IFAC World Congress in 2014 and PC member of the forthcoming DCDS 2015 conference.

9.2.3. Journal

9.2.3.1. reviewer

Éric Badouel is reviewer for AMS (MathSciNet) and reviewed papers for Science of Computer Programming, Fundamenta Informaticae, Theoretical Computer Science, and Transaction on Petri Nets and Other Models of Concurrency.

Nathalie Bertrand has written reviews for Logical Methods in Computer Science, Information Processing Letters, Information and Computation.

Éric Fabre is a regular reviewer for the Ministry of Education and Research, through the Credit Impot Recherche program (support to industrial research through tax reductions). He reviewed for several journals and conferences: Automatica, Journal of discrete event dynamical systems, CDC, ACC,...

Hervé Marchand was this year reviewer for Automatica and Journal of discrete event dynamical systems.

Thierry Jérón was reviewer for Annals of telecommunications, Evolving Systems, Science of Computer Programming and Software Testing, Verification and Reliability.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Christophe Morvan

License: Compilation, System, Advanced Algorithmics Université de Paris-Est, Marne-la-Vallée, France.

Nathalie Bertrand

Agreg: Responsible of computer science organization, 16h (eq. TD), M2, Ecole Normale Supérieure de Rennes, France.

Loïc Héluët

Licence: JAVA programming, 35h, INSA Rennes, France.

Agreg: Algorithms, M2, ENS Rennes, France.

Master: Initiation to research, M1, ENS Rennes, France.

Éric Fabre

Master: "ASR: introduction to distributed systems and algorithms," 12h (eq. TD), M2, Univ. Rennes 1, France.

Master: "Information theory," 30h (eq. TD), M1, Ecole Normale Supérieure de Rennes, France.

Master: Preparation of Agrégation, 6h (eq. TD), M1, Ecole Normale Supérieure de Rennes, France.

Master: Initiation to research, 12h (eq. TD), M1, ENS Rennes, France.

Licence : "Information theory for computer scientists," 4.5h (eq. TD), L3, Ecole Normale Supérieure de Cachan, France.

9.3.2. Supervision

HdR: Christophe Morvan, Familles de graphes de présentation finie, propriétés et applications, Université de Paris-Est Marne-La-Vallée, 19 novembre 2014.

PhD: Sébastien Chédor, *Diagnostic, opacité et test de conformité pour des systèmes récursifs*, Université Rennes 1, 7th january 2015, supervised by Thierry Jérón and Christophe Morvan.

PhD: Mohamadou Lamine Diouf, *Opacité des artefacts d'un système workflow*, Rennes I University and University Cheikh Anta Diop (UCAD) in Dakar, 10th October 2014, supervised by Éric Badouel.

PhD in progress: Srinivas Pinisetty, *Runtime validation of critical control-command systems*, started in December 2011, supervised by Thierry Jérón and Hervé Marchand. Defense scheduled 23rd of January 2015.

PhD in progress: Bruno Karelavic, *Approximated analysis for checking Stochastic Models and Games*, started in November 2012, supervised by Blaise Genest and Wieslaw Zielonka.

PhD in progress : Paulin Fournier, *Parameterized verification of networks of probabilistic processes*, started in september 2012, supervised by Nathalie Bertrand and Thierry Jérón.

PhD in progress: Mathieu Pichene, Stochastic models to model apoptosis, started in December 2014, supervised by Blaise Genest.

PhD in progress: Karim Kecir, *Supervision of urban railway systems with advanced regulation techniques*, starting early 2015 (currently in pre-thesis period before a CIFRE convention is agreed by the ANRT), supervised by Loïc Hérouët.

9.3.3. Juries

Nathalie Bertrand was member of the private and public PhD defenses committee of Aaron Bohy, *Antichain based algorithms for the synthesis of reactive systems*, Université Mons, Belgium, 30/05/2014 and 10/06/2014.

This year, Thierry Jérôme has been:

- member of the PhD defense jury of Axel Belinfante, *JTorX: Exploring Model-based Testing*, University of Twente, Netherlands, 18/09/2014.
- member and president of the PhD defense jury of Hernan Ponce de Léon, *Testing concurrent systems through event structures*, LSV, ENS Cachan, 7/11/2014.
- member and president of the PhD defense jury of Anaïs Guignard, *Validation fonctionnelle de contrôleurs logiques: contribution au test de conformité et à l'analyse en boucle fermée*, Lurpa, ENS Cachan, 4/12/2014.

Éric Fabre participated to the Habilitation committee (HDR) of Samy Abbes, University Paris Diderot (Paris 7), "Asynchronous Probabilistic Processes," Sept. 2014.

TEMPO Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events

8.1.1.1. Invitationr

Vania Joloboff was invited for a short stay at Academia Sinica in Taipei Taiwan, in October 2014.

8.1.1.2. Member of the organizing committee

Vania Joloboff jointly organized with ECNU staff the LIAMA Open Day in Shanghai in July 2014

Vania Joloboff jointly organized and chaired a session at the LIAMA Workshop for collaboration between Europe and China in May 2014.

Mingsong Chen was invited to served as a Session Chair of the conference SERE 2015.

8.1.1.3. Member of the conference program committee

Vania Joloboff is program committee member of DATE conference workshop on Model Implementation Fidelity.

Mingsong Chen served as a Program Committee member of International Conference on VLSI Design.

Mingsong Chen served as a Program Committee member of the conference SAC 2015.

Mingsong Chen served as a Program Committee member of the conference DATE 2015.

8.1.1.4. Reviewer

Mingsong Chen was a reviewer for the conferences VLSID 2015, SAC 2015, DATE 2015, DAC 2015.

8.1.2. Journal

8.1.2.1. Member of the editorial board

Mingsong Chen serves as an associate editor of Journal of Circuits, Systems and Computers.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Virtual Prototyping

Vania Joloboff : Virtual Prototyping, ECNU SEI

Master Students

8.2.2. Supervision

Mingsong Cheng and Vania Joloboff started supervision of several Master and PhD. students at East China Normal University.

8.2.3. Juries

Vania Joloboff was jury member of PhD defence for Yanwen Chen, a double PhD degree of East China Normal University and University of Nice.

TOCCATA Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- J.-C. Filliâtre chaired the fifth meeting of the IFIP Working Group 1.9/2.15 (Verified Software) in Vienna, Austria, July 2014.

9.1.1.2. Member of the organizing committee

- S. Boldo and G. Melquiond are members of the organizing committee for the 22nd IEEE Symposium on Computer Arithmetic (ARITH 2015), held in Lyon in June 2015.
- J.-C. Filliâtre organized the sixth meeting of the IFIP Working Group 1.9/2.15 (Verified Software) in Paris, France, December 2014.
- C. Paulin co-organized with Z. Shao (Harvard University) the *Workshop on certification of high-level and low-level programs*, July 7-11, 2014. This workshop was part of the IHP thematic trimester *Semantics of proofs and certified mathematics*, which took place in Paris from April to July.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committee

- S. Boldo is a member of the program committee of the 7th International Workshop on Numerical Software Verification (NSV-7). For 2015, she will be in the program committees of the 26th Journées Francophones des Langages Applicatifs (JFLA 2015), of the 8th International Workshop on Numerical Software Verification (NSV-8) and of the 22nd IEEE Symposium on Computer Arithmetic (ARITH 2015).
- A. Charguéraud served on the external review committee for POPL 2015.
- É. Contejean is a member of the program committee of the ACM SIGPLAN 2014 Workshop on Partial Evaluation and Program Manipulation, (PEPM 2014) affiliated with the POPL 2014 conference.
- J.-C. Filliâtre is a member of the program committees of the Symposium on Languages, Applications and Technologies (SLATE 2014) and the Journées Francophones des Langages Applicatifs (JFLA 2014).
- C. Marché, member of program committee of the first international workshop Formal-IDE (F-IDE), held as a satellite workshop of ETAPS 2014 <http://perso.ensta-paristech.fr/~etaps/>, and of the next workshop F-IDE 2015.
- C. Paulin is a member of the program committees of the conference Interactive Theorem Proving (ITP 2014) and the Coq Workshop 2014. For 2015, she will be in the program committees of the following conferences: Certified Programs and Proofs (CPP 2015), Mathematics of Program Construction (MPC 2015) and Types for Proofs and Programs (TYPES 2015).
- A. Paskevich is a member of the program committee of the 11th International Workshop on User Interfaces for Theorem Provers (UITP 2014) affiliated with the FLoC 2014 conference.

9.1.2.2. Reviewer

The members of the Toccata team have reviewed papers for numerous international conferences, including: ARITH, CICM, CPP, ESOP, NFM, POPL, SLATE.

9.1.3. Journal

9.1.3.1. Member of the editorial board

- S. Boldo is member of the editorial committee of the popular science web site “i()”: <http://interstices.info/>.
- S. Boldo is member of the editorial board of Binaire <http://binaire.blog.lemonde.fr>, the blog of the French Computer Science Society.
- J.-C. Filliâtre is member of the editorial board of the *Journal of Functional Programming*.
- C. Paulin is member of the editorial board of the *Journal of Formalized Reasoning*.

9.1.3.2. Reviewer

The members of the Toccata team reviewed numerous papers for numerous international journals, including: Journal of Automated Reasoning (JAR), Transactions in Computational Sciences (TCS), Theory of Computing Systems (TCS), IEEE Transactions on Computers (TC), Journal of Scientific Programming, Journal of Field Robotics (JFR), Mathematical Structures in Computer Science (MSCS), Journal of Automated Software Engineering.

9.1.4. Invited Talks

- S. Boldo was invited speaker at the 16th GAMM-IMACS International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics conference (SCAN 2014) [25] about her methodology for the formal verification of floating-point programs.
- S. Boldo and G. Melquiond were invited speakers at an international workshop in Lyon, France called Mathematical Structures of Computation during the week 4: Formal Proof, Symbolic Computation and Computer Arithmetic. <http://smc2014.univ-lyon1.fr/doku.php?id=week4>.
- C. Lelay was invited speaker at the 25th JFLA (Journées Francophones des Langages Applicatifs), Fréjus, France, Jan 10th, 2014 about “Coq passe le bac”: she tried the 2013 mathematics test of the scientific Baccalaureate in Coq at the same time as the students.
- C. Marché, “Calcul de plus faible précondition, revisité en Why3”, 25th JFLA, special session on selected representative papers of past editions, joint work with A. Tafat, Fréjus, France, Jan 11th, 2014.
- C. Marché, “Beyond SPARK2014: the ProofInUse project”, IFIP WG1.9/2.15, Vienna, Austria, Jul 15th, 2014.
- G. Melquiond was invited speaker at the 12th International Workshop on Satisfiability Modulo Theories (SMT 2014).
- C. Paulin was invited speaker at the 25th JFLA (Journées Francophones des Langages Applicatifs), Fréjus, France, Jan 10th, 2014 to give a tutorial presentation of the ALEA library. She also gave an invited talk during the GDR-GPL “Journées Nationales”.
- C. Paulin was invited speaker at the workshop “All about Proofs, Proofs for All” (APPA) as part of the Vienna Summer of Logic. She presented an introduction to the Calculus of Inductive Constructions. She wrote a chapter in the post-conference book [115] to appear next year.

9.1.5. Collective Responsibilities

- S. Boldo, elected member of the Inria Evaluation Committee until August 2014. She was in the committee in charge of selecting the Inria permanent researchers (CR2) in Bordeaux and Nancy and in the national committee for first-class Inria permanent researchers (CR1).
- S. Boldo, member of the national Inria admission committee.
- S. Boldo, C. Marché, and G. Melquiond, members of committees in charge of recruiting assistant professors at Université Paris-Sud.
- S. Boldo, member of the CLFP, *comité local de formation permanente*.

- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- S. Boldo, member of the national popularization committee, *comité de médiation scientifique*, of 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 (IOI). France-ioi also provides online exercises in programming and algorithmics—in average, over 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.
- A. Charguéraud and G. Melquiond are members of the committee for the monitoring of PhD students (*commission de suivi des doctorants*).
- S. Conchon and A. Paskevich, members of the *commission consultative de spécialistes de l'université*, Section 27, University Paris-Sud since December 2014.
- É. Contejean, leader of the VALS team since February 2014.
- É. Contejean, nominated member of the *conseil du laboratoire* of LRI since April 2010 till June 2014.
- É. Contejean, elected member of the *section 6 du Comité National de la Recherche Scientifique* since September 2012.
- É. Contejean, member of the committee of experts for the AERES evaluation of the Verimag laboratory (2014).
- É. Contejean, reviewer for the ANR (2014).
- É. Contejean, reviewer for the START program of the Austrian Science Fund (FWF) (2014).
- S. Dumbrava, elected member of the *conseil du laboratoire* of LRI since June 2014.
- 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.
- C. Lelay, elected member of the *conseil du laboratoire* of LRI from November 2011 to June 2014.
- C. Marché and S. Boldo, members of the *jury de l'agrégation externe de mathématiques* as experts in computer science, since 2012.
- 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, member of the executive team of the LRI (as “chargé de mission”), since July 2014.
- C. Marché, president of the hiring committee of one associate professor position (Maître de Conférences), Université Paris-Sud, April-June 2014. Member of another such committee.
- C. Marché, director of the ProofInUse Joint Laboratory between Inria and AdaCore, <http://www.spark-2014.org/proofinuse>
- G. Melquiond and C. Paulin, members of the *commission consultative de spécialistes de l'université*, Section 27, University Paris-Sud since April 2010. C. Paulin is the president of this committee since December 2014.
- 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.
- C. Paulin, chaired the hiring committee for a professor position in computer science at Université Paris-Sud.
- In 2014, C. Paulin was elected member of the Informatics Section of Academia Europaea <http://www.ae-info.org/>.
- A. Paskevich was 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 till August 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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), A. Charguéraud (12h), Université Paris 7, France.

Licence: “Programmation Fonctionnelle avancée” (L3), M. Clochard (10h), Université Paris-Sud, France.

Master: “Projet de programmation (compilation)” (M1), M. Clochard (50h), Université Paris-Sud, France.

Licence: “Programmation fonctionnelle avancée” (L3), S. Conchon (30h), Université Paris-Sud, France.

Master: “Compilation” (M1), S. Conchon (33h), Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): “Systèmes” (S3), D. Declerck, IUT d’Orsay, Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): “Programmation et administration des bases de données” (S2), S. Dumbrava (62h), IUT d’Orsay, Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): “Bases de données avancées” (S3), S. Dumbrava (36h), IUT d’Orsay, Université Paris-Sud, France.

Licence: “Langages de programmation et compilation” (L3), J.-C. Filliâtre (36h), École Normale Supérieure, France.

Licence: “INF411: Les bases de l’algorithmique et de la programmation” (L3), J.-C. Filliâtre (16h), École Polytechnique, France.

Licence: “Mathématiques pour l’informatique” (L2), L. Gondelman (30h), Université Paris-Sud, France.

Master: “Compilation” (M1), L. Gondelman (28h), Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): “Programmation système” (S4), A. Paskevich (48h), IUT d’Orsay, Université Paris-Sud, France.

9.2.2. Internships

- Y. Chatelain, a L3 student from Université Paris-Sud, did a 2-month internship under the supervision of J.-C. Filliâtre and A. Paskevich, on the implementation of a new criterion of termination of recursive functions in a pure functional language.
- J.-P. Deplaix, a third-year student of Epitech, did a 4-month internship, supervised by J.-C. Filliâtre and A. Paskevich, on the compilation of *Why3* programs to C.

- J. Grangier, a M1 student from ENSIEE, did a 10-week internship under the supervision of A. Charguéraud, on the verification of the functional correctness and the asymptotic complexity of a dynamic array data structure.
- X. Onfroy, a L3 student from ENS-Lyon, did a 6-week internship, supervised by G. Melquiond, on the formalization of the gauge integral in the setting of the Coquelicot library.

9.2.3. Supervision

HDR: É. Contejean, “Facettes de la preuve, Jeux de reflets entre démonstration automatique et preuve assistée” [13], Université Paris-Sud, June 13th, 2014.

HDR: S. Boldo, “Deductive Formal Verification: How To Make Your Floating-Point Programs Behave” [12], Université Paris-Sud, October 6th, 2014.

PhD: C. Dross, “Theories and Techniques for Automated Proof of programs” [14], Université Paris-Sud, Apr. 1st, 2014, supervised by C. Marché, A. Paskevich, and with industrial supervisors Y. Moy and J. Kanig (AdaCore company).

PhD: A. Mebsout, “SMT-based Model-Checking” [15], Université Paris-Sud, Sep. 29th, 2014, supervised by F. Zaïdi (LRI) and S. Conchon.

PhD in progress: C. Lelay, “Real numbers for the Coq proof assistant”, since Oct. 2011, supervised by S. Boldo and G. Melquiond.

PhD in progress: S. Dumbrava, “Towards data certification”, since Oct. 2012, supervised by V. Benzaken (LRI) and É. Contejean.

PhD in progress: L. Gondelmans, “Obtention de programmes corrects par raffinement dans un langage de haut niveau”, since Oct. 2013, supervised by J.-C. Filliâtre and A. Paskevich.

PhD in progress: M. Clochard, “A unique language for developing programs and prove them at the same time”, since Oct. 2013, supervised by C. Marché and A. Paskevich.

PhD in progress: J. C. Mbiada Djanda, “Augmented Semantics for the Non-interference of critical C Code”, since Nov. 2013, supervised by C. Marché and J. Signoles (CEA LIST).

PhD in progress: D. Declerck, “Vérification par des techniques de test et model checking de programmes C11”, since Sep. 2014, supervised by F. Zaïdi (LRI) and S. Conchon.

9.2.4. Juries

S. Boldo: examiner, PhD committee of Mohamed Amine Najahi, “Synthesis of certified programs in fixed-point arithmetic, and its application to linear algebra basic blocks”, Perpignan, France, December 2014.

J.-C. Filliâtre: examiner, PhD committee of Jonathan Protzenko, “Mezzo: the language of the future”, Université Paris Diderot, September 2014.

C. Marché: reviewer, PhD committee of T. Bormer “Advancing Deductive Program-Level Verification for Real-World Application”, Karlsruhe Institute of Technology, Karlsruhe, Germany, October 2014.

C. Marché: examiner, HDR committee of S. Boldo, “Deductive Formal Verification: How To Make Your Floating-Point Programs Behave”, Université Paris-Sud, October 2014.

C. Paulin: examiner, PhD committee of Guillaume Cano, “Interaction entre algèbre linéaire et analyse en formalisation des mathématiques”, University of Nice-Sophia Antipolis, March 2014.

C. Paulin: examiner, HDR committee of Évelyne Contejean, “Facettes de la preuve, Jeux de reflets entre démonstration automatique et preuve assistée”, Université Paris-Sud, June 2014.

C. Paulin: president of the PhD committee of Peva Blanchard “Synchronization and Fault-tolerance in Distributed Algorithms”, Université Paris-Sud, September 2014.

C. Paulin: examiner, HDR committee of Stéphane Graham-Lengrand “Polarities & Focussing: a Journey from Realisability to Automated Reasoning”, Université Paris-Sud, December 2014.

9.3. Popularization

- S. Boldo presented the *Concours Castor informatique* to computer sciences teachers (ISN) in Nancy on April 17th, 2014. A video of the talk is available at <http://videos.univ-lorraine.fr/index.php?act=view&id=1369>.
- S. Boldo gave a 2-hour course entitled *Les nombres et l'ordinateur* at the École Normale Supérieure de Cachan, France, on September 9th.
- S. Boldo gave a 2-hour course *Pourquoi mon ordinateur calcule faux?* to a general audience at the Université Inter-Âge in Versailles, France, on March 4th.
- S. Boldo gave a talk for computer sciences teachers (ISN) in Créteil on March 24th
- S. Boldo gave a talk for teenagers at the lycée Maximilien Perretin Alfortville on May 22nd.
- S. Boldo wrote an article with Jean-Michel Muller (ARIC) in the popularization journal *La Recherche* [42].
- S. Boldo wrote in 2013 an article for the French blog celebrating 2013 as the “Mathematics of Planet Earth” year: <http://mpt2013.fr/meme-les-ordinateurs-font-des-erreurs/>. This article was selected to be published in a book published in 2014 [41].
- S. Boldo is member of the editorial committee of the popular science Interstices web site, since April 2008. <http://interstices.info/>.
- S. Boldo is member of the editorial board of *Binaire* <http://binaire.blog.lemonde.fr>, the blog of the French Computer Science Society.
- S. Boldo, G. Melquiond, A. Paskevich, and C. Paulin animated two stands at the *Fête de la science*.
- A. Charguéraud and S. Boldo contributed to the preparation of the exercises of the *Concours Castor informatique* <http://castor-informatique.fr/>. A. Charguéraud is also one of the three organizers of this contest. The purpose of the *Concours Castor* is to introduce pupils (from *6ème* to *terminale*) to computer sciences. More than 228,000 teenagers played with the interactive exercises in November 2014.
- S. Conchon and J.-C. Filliâtre published a book “*Apprendre à programmer avec OCaml*” for undergraduate students learning computer programming [39] (Eyrolles, September 2014).

VERIDIS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Organization of scientific events

9.1.1.1. General Chair, Scientific Chair

Pascal Fontaine co-organized the SAT/SMT Summer School 2014, affiliated with Vienna Summer of Logic, in Semmering, Austria.

Stephan Merz is a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS). He co-organized the TLA⁺ Community Event, a satellite of ABZ 2014 in June in Toulouse.

Thomas Sturm is chair of the steering committee of the conference series *Mathematical Aspects of Computer and Information Sciences* (MACIS). He coordinated the CDZ Workshop GZ1115 *Computation and Reasoning with Constraints*, Beijing, China, 2014.

Christoph Weidenbach is a member of the steering committee of *Bundeswettbewerb Informatik*, the German competition among high-school students in computer science.

9.1.1.2. Membership in Organizing Committees

The International Summer School on Verification Techniques, Systems, and Applications (VTSA) has been organized since 2008 in the Greater Region (Nancy, Saarbrücken, Luxembourg, and Liège), and Stephan Merz and Christoph Weidenbach are co-organizers of VTSA. In 2014, VTSA took place during the last week of October in Luxembourg.

9.1.2. Service in Program Committees

9.1.2.1. Chairmanship of Conference Program Committees

Dominique Méry was co-chair of the program committee of the 11th International Colloquium on Theoretical Aspects of Computing, held in Bucharest, Romania in September, and of the First Workshop on Formal Integrated Development Environments, a satellite of ETAPS in Grenoble, France, in April.

Stephan Merz was co-chair of the program committee of the 16th International Conference on Formal Engineering Methods, held in Luxembourg in November, and of the First International Workshop on Formal Reasoning in Distributed Algorithms (FRIDA) in July, as part of Vienna Summer of Logic.

Christoph Weidenbach was co-chair of the program committee for the 7th International Joint Conference on Automated Reasoning (IJCAR) that took place in Vienna, Austria, as part of Vienna Summer of Logic.

9.1.2.2. Membership in Conference Program Committees

Pascal Fontaine served on the program committees of the International Joint Conference on Automated Reasoning (IJCAR) and of the workshops PAAR and SMT.

Dominique Méry served on the program committees of ABZ, AFADL, CSDM, MedicalCPS, FHIES, FM, ICFEM, iFM, and FACS.

Stephan Merz served on the program committees of the international conferences ABZ, IJCAR, SAC, SEFM, SSS, and of the workshops AVoCS, GRSRD, SETS, and VERIFY.

Uwe Waldmann served on the program committee of IJCAR.

9.1.3. Journal Edition

Stephan Merz (together with Gerald Lüttgen of University of Bamberg) edited a special issue of *Science of Computer Programming* on the Automated Verification of Critical Systems, following AVoCS 2012.

Thomas Sturm is a member of the editorial boards of the *Journal of Symbolic Computation* (Elsevier) and *Mathematics in Computer Science* (Springer).

Christoph Weidenbach is an editor of the Journal of Automated Reasoning.

9.1.4. Scientific Bodies and Self-Administration

Pascal Fontaine was an elected member of the SMT Steering Committee (2012–2014), and he is one of three SMT-LIB managers. He was elected CADE trustee in October 2014.

Dominique Méry is a member of the IFIP Working Group 1.3 on *Foundations of System Specification*. He is the head of the Doctoral School IAEM Lorraine for the University of Lorraine and head of the Formal Methods department of the LORIA laboratory. He is an expert for the French Ministry of Education (DS9), an expert for the French Agence Nationale de la Recherche (ANR) and for AERES.

Stephan Merz is a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*. He is a member of the Scientific Directorate of the International Computer Science Meeting Center in Schloss Dagstuhl. He is the delegate for the organization of conferences at the Inria Nancy Grand Est research center and co-head of the PhD committee for computer science in Lorraine. He was a member of the hiring committee for an associated professor at Université Toulouse 3 and an expert for Agence Nationale de la Recherche (ANR), for Haut Conseil de l'Évaluation de la Recherche et de l'Enseignement Supérieur (HCERES), for the German DFG, the Dutch NWO, and for the European Research Council (ERC).

Thomas Sturm is a member of the selection committee for MSc and PhD students at the International Max Planck Research School.

Christoph Weidenbach is a trustee of CADE (elected 2009, reelected 2012). He is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

The university employees of VeriDis (in Nancy) have statutory teaching obligations of 192 hours per year. We indicate the graduate courses that members of the team have been teaching in 2014.

Marie Dufлот-Kremer taught a course on Introduction to Algorithmic Verification (first-year master level at Université de Lorraine). She and Stephan Merz also taught a course on Algorithmic Verification in the second year of master and for students of Erasmus Mundus Dependable Software Systems.

Pascal Fontaine is head of the Master MIAGE (Business Informatics) at Université de Lorraine since September 2014.

Stephan Merz taught a course on formal specification using TLA⁺ at the SPES_XT summer school on model-based development of embedded systems at the University of Twente (The Netherlands) in September.

Uwe Waldmann gave courses on Automated Reasoning I and II at Saarland University.

Christoph Weidenbach gave a course on Automated Reasoning I.

9.2.2. Supervision

PhD: Arnaud Fietzke, Labelled Superposition, Universität des Saarlandes. Supervised by Christoph Weidenbach, defended on June 5, 2014.

PhD: Hernán Pablo Vanzetto, Proof Automation and Type Synthesis for Set Theory in the Context of TLA⁺, Université de Lorraine. Supervised by Kaustuv Chaudhuri and Stephan Merz, defended on December 8, 2014.

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 Stephan Merz and Christoph Weidenbach, since 11/2012.

PhD in progress: Haniel Barbosa, Refutational Completeness in Satisfiability Modulo Theories, Université de Lorraine and UFRN (Natal, Brazil). Supervised by David Déharbe, Pascal Fontaine, and Stephan Merz, since 12/2013.

PhD in progress: Martin Bromberger, Arithmetic Reasoning, Saarland University. Supervised by Christoph Weidenbach, since 07/2014.

PhD in progress: Pablo Federico Dobal, Satisfiability Modulo Arithmetic Theories, Université de Lorraine and Saarland University. Supervised by Pascal Fontaine, Stephan Merz, and Thomas Sturm, since 09/2014.

PhD in progress: Marek Košta, Computational Logic, Universität des Saarlandes. Supervised by Thomas Sturm, since 11/2011.

PhD in progress: Manuel Lamotte Schubert, Automatic Authorization Analysis, Saarland University. Supervised by Christoph Weidenbach, 07/2010.

PhD in progress: Marco Voigt, Decidable Hierarchic Combinations, Saarland University. Supervised by Christoph Weidenbach, since 11/2013.

PhD in progress: Daniel Wand, First-Order Extensions to Support Higher-Order Reasoning, Saarland University. Supervised by Christoph Weidenbach, since 02/2011.

9.2.3. Juries

Stephan Merz served as a reviewer for the PhD theses of Nadezhda Baklanova (Univ. Toulouse 3), Claire Dross (Univ. Paris Sud), and Giuliano Losa (EPFL Lausanne).

9.3. Popularization

Marie Duflot-Kremer took part in various popularization activities, with a public ranging from primary school kids (with unplugged activities concerning sorting, programming, error detection) to non-scientific staff of the Inria center. She is also a member of the steering committee preparing an itinerant exposition intended for explaining computer science to high-school students and took part in an event of the European Code Week in Paris.

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

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

CARTE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

The Carte Team has organized a few conferences and workshops in Nancy this year:

- **Journées SDA2 and FRAC 2014**, April.
- JFIN (Journée Française d'investigation numérique), October.
- Botconf'14 (The botnet fighting conference - Second edition), December.

Simon Perdrix organised JIQ'14 (Journées Informatique quantique) in Lyon in November.

8.1.2. Scientific events selection

8.1.2.1. Conference program committee membership

- Guillaume Bonfante was in the Program Committee of the conference FPS (Foundations and Practice of Security) and the following workshops: Termgraph (Vienna), Caesar (Rennes), PPREW (New Orleans).
- Mathieu Hoyrup was in the Program Committee of Computability and Complexity in Analysis (CCA) 2014.
- Romain Péchoux was in the Program Committee of DICE 2014 (Developpements in Implicit Computational complExity).
- Simon Perdrix was in the Program Committee of STACS 2014 (Symposium on Theoretical Aspects of Computer Science) and QPL 2014 (Quantum Physics and Logic).

8.1.2.2. Reviewing activities

- Mathieu Hoyrup reviewed articles for LICS 2014, CiE 2014.
- Emmanuel Jeandel reviewed articles for STACS 2015.
- Romain Péchoux reviewed articles for DICE 2014 (Developpements in Implicit Computational complExity), ISMVL 2015 (International Symposium on Multi-Valued Logics), RTA-TLCA 014 (Rewriting Techniques and Applications - Typed Lambda-Calculi and Applications).
- Simon Perdrix reviewed articles for CONCUR'14.

8.1.3. Journal

8.1.3.1. Editorial board membership

- Emmanuel Jeandel is in the editorial board of **RAIRO-ITA**.

8.1.3.2. Reviewing activities

- Mathieu Hoyrup reviewed articles for *Theory of Computing Systems*, *Logical Methods in Computer Science*, *Mathematical Structures in Computer Science*.
- Emmanuel Jeandel reviewed articles for *Journal of Computer and System Sciences* and for *Ergodic Theory and Dynamical Systems*.
- Simon Perdrix reviewed articles for *Information Processing Letters*, *Quantum Information & Computation*.

8.1.4. Invited Talks

- Jean-Yves Marion gave an invited talk at the Journées Francophones de l'Investigation Numérique (JFIN).
- Emmanuel Jeandel gave an invited talk at the Journées Montoises.
- Simon Perdrix gave an invited talk at the Workshop on Quantum Metrology, Interaction, and Causal Structure 2014 (Tsinghua University, Beijing) and an invited talk at the Chinese Academy of Sciences.

8.1.5. Collective Responsibilities

Isabelle Gnaedig is:

- member of the scientific mediation committee of Inria Nancy - Grand Est,
- researcher social referee at Inria Nancy - Grand Est.

Simon Perdrix is responsible of GT IQ (groupe de travail Informatique quantique) at the CNRS GdR IM (groupe de recherche Informatique Mathématique).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence :

- Guillaume Bonfante
 - Java, L3, Mines Nancy
- Emmanuel Hainry
 - Operating Systems, 30h, L1, IUT Nancy Brabois
 - Algorithmics, 40h, L1, IUT Nancy Brabois
 - Dynamic Web, 60h, L1, IUT Nancy Brabois
 - Databases, 30h, L1, IUT Nancy Brabois
 - Object Oriented Languages, 12h, L2, IUT Nancy Brabois
 - Complexity, 30h, L2, IUT Nancy Brabois
- Mathieu Hoyrup
 - Programmation en JAVA, 56h, DUT d'informatique 1ère année, IUT Charlemagne, France
- Emmanuel Jeandel
 - Algorithmics and Programming 1, 60h, L1 Maths-Info
 - Algorithmics and Programming 4, 30h, L3 Informatique
 - Modelling Using Graph Theory, 30h, L3 Informatique
 - Networking, 15h, L3 Informatique
- Romain Péchoux
 - Programmation orientée objet, 37,5h, L3, Université de Lorraine, France
 - Programmation orientée objet, 33,5h, L2, Université de Lorraine, France
 - Outils logiques pour l'informatique, 25h, L1, Université de Lorraine, France
 - Bases de données, 42h, L3, Université de Lorraine, France
 - Algorithmic complexity, 30h, L3 MIASHS parcours MIAGE, IGA Casablanca, Marocco.
- Simon Perdrix
 - Structure de données, 72h, DUT d'informatique 1ère année, IUT Charlemagne, France

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, 20h, M2, Telecom-Nancy
- Emmanuel Jeandel
 - Algorithmics and Complexity, M1 Informatique and M1 ENSEM, 30h
 - Combinatorial Optimization, M1 Informatique, 36h.
- Romain Péchoux
 - Mathematics for computer science, 30h, M1 SC
 - Advanced Java, 52,5h, M1 MIAGE
- Simon Perdrix
 - Pépites Algorithmiques — Informatique Quantique, 6h, M1/M2, Ecole des Mines de Nancy.

8.2.2. Supervision

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 : Hugo Férée, Complexité d'ordre supérieur et analyse récursive, Université de Lorraine, 10 December 2014, Jean-Yves Marion and Mathieu Hoyrup.

PhD in progress: Hubert Godfroy, Semantics of Self-modifying Programs, Jean-Yves Marion.

PhD: Jérôme Javelle, Quantum Cryptography: Protocols and Graphs, June 2nd 2014, 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.

8.2.3. Juries

Isabelle Gnaedig was a:

- member of the Inria hiring committee for young researchers,
- member of the Telecom-Nancy engineering school admission committee.

Emmanuel Jeandel was in the:

- Selection committee for a research assistant position in Nice (MCF 1313).
- Selection committee for a professor position in Marseille (PR 174).
- Jury of Jérôme Javelle's PhD Defense on "Cryptographie Quantique: Protocoles et Graphes", defended in Université de Grenoble, June 2nd.
- Jury of Benjamin Hellouin de Menibus's PhD Defense on "Asymptotic Behaviour of Cellular Automata: Computation and Randomness", defended in Aix-Marseille Université, September 26th.
- Jury of Bastien Le Gloannec's PhD Defense on "Coloriage du plan discret par jeux de tuiles déterministes", defended in Université d'Orléans, December 12th.

8.3. 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.

CASSIS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting⁰. These recommendations influence the design of e-voting systems that are deployed in France. However, some of the recommendations seem a bit outdated and dedicated to particular classes of systems. Even more importantly, the CNIL recommendations focus on vote privacy but do not say much about verifiability. Véronique Cortier, David Galindo, and Stéphane Glondu have formulated new recommendations, submitted to the CNIL. They have met some CNIL members to discuss how to integrate some of the propositions to the new version of the CNIL recommendations that should appear in 2015.

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Véronique Cortier: FMS 2014, 5th Workshop on Formal Methods for Security.
Christophe Ringeissen: UNIF 2014, 28th International Workshop on Unification.

9.1.2. Scientific Events Selection

9.1.2.1. Program Committee Chair

- Steve Kremer: Post 2014, ACM SEC@SAC 2014, GRSRD'15

9.1.2.2. Program Committee Member

- Véronique Cortier: ACNS 2014, CCS 2014, Esorics 2014, FCC-FCS 2014, FoSSaCs 2014, Icalp 2014, Movep 2014, Concur 2015, LICS 2015, POST 2015.
- Christophe Ringeissen: CADE-25, FroCoS 2015.
- Frédéric Dadeau : CSTVA 2014, NFM 2014, QSIC 2014.
- Abdessamad Imine : AICCSA 2014, DEXA 2014, DEXA 2015, ICEIS 2015, DASFAA 2015
- Steve Kremer : ACNS 2014, ICFEM 2014, AsiaCCS 2015, ESORICS 2015, FCS 2015, TGC 2015.
- Michaël Rusinowitch: LATA 2014, CRISIS 2014, STP 2014, GRSRD 2014, TGC 2015, POST 2016.
- Fabrice Bouquet : ICST 2014, MoDeVva 2014, AMOST 2015

9.1.3. Journal

9.1.3.1. Editorial Board Member

- Véronique Cortier: Information & Computation, Journal of Computer Security.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Summer School:
Fabrice Bouquet, Test techniques and validation for Software, ENVOL 2014, Organized by: CNRS, INRA, VetAgro-Sup and Inria, November 18-21, 2014 (<https://www.projet-plume.org/envol-2014>)
Steve Kremer, Formal Modeling and Automated Analysis of Security Protocols, 14th International School on Foundations of Security Analysis and Design (FOSAD'14)

⁰<http://www.cnil.fr/documentation/deliberations/deliberation/accessible/non/delib/249/>

- Master:
 - Fabrice Bouquet, Functional Testing, 18 hours, M2 Computer science, Franche-Comté University, France.
 - Fabrice Bouquet, Artificial Intelligence, 42 hours, M1 Computer science, Franche-Comté University, France.
 - Frédéric Dadeau, Structural testing, 9 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Alain Giorgetti, Program Proofs, 58 hours, M1 Computer science, Franche-Comté University, France.
 - Alain Giorgetti, Decision Procedures, 13 hours, M2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Security and Components, 10,5 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.
 - Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, 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, 22.5 hours (ETD), M2 Computer science, Lorraine University, France.
 - Laurent Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Lorraine University, France.
- Licence:
 - Alain Giorgetti, Logics and Deduction, 52 hours, L2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Formal Languages, 65 hours (ETD), L3 Computer science, Franche-Comté University, France.
- E-Learning:
 - Fabrice Bouquet, Artificial Intelligence, 78 (ETD), M1 Computer science, Franche-Comté University, France.
 - Fabrice Bouquet, Specification Validation and Test, 39 (ETD), M2 Computer science, Franche-Comté University, France.
 - Alain Giorgetti, Formal Methods, 81 hours, L3 computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2 Computer science, Franche-Comté University, France.

9.2.2. Supervision

- PhD (defended in 2014):
 - Robert Künnemann, Verification of Security APIs, January 7, Steve Kremer and Graham Steel

Houari Mahfoud, Access Control Models for XML Documents, February 18, Abdessamad Imine and Michaël Rusinowitch

Cyrille Wiedling, Formal analysis of E-voting protocols, November 21, Véronique Cortier

Ivan Enderlin, Test Data Generation for Unit Testing in PHP, July 16, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

Aloïs Dreyfus, Contribution to the efficient model-based verification and testing, October 22, Pierre-Cyrille Héam and Olga Kouchnarenko

Bin Yang, Contribution to a kernel of a symbolic asymptotic modeling software, December 16, Michel Lenczner and Alain Giorgetti

- 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

Maxime Bride, Automated Synthesis and Verification of Security Services, started in October 2014, Michaël Rusinowitch

Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune

Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on micro-systems, 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

Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, Véronique Cortier

Huu Hiep Nguyen, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Steve Kremer

Guillaume Scerri, Symbolic and automatic security proofs in computational models, started in September 2011, Hubert Comon-Lundh and Véronique Cortier

9.2.3. Juries

Inria evaluation committee (Véronique Cortier, Steve Kremer, Michaël Rusinowitch)

Vice-president of the Jury Junior Research Position Inria Nancy Grand Est (Véronique Cortier)

Jury Junior Research Position Inria Paris-Rocquencourt (Véronique Cortier)

Preselection Jury for Inria Advanced and Starting Research Positions (Michaël Rusinowitch)

Member of the ANR scientific evaluation committee, challenges 7 and 9 (Olga Kouchnarenko)

Examiner for Guillaume Laville PhD, Besançon, June 27, 2014, *Exécution efficace de systèmes multi-agents sur GPU* (Fabrice Bouquet)

Reviewer for Maxime Fonda PhD, Bourges, May 21, 2014, *Protection obligatoire des serveurs d'application web : application aux processus métiers* (Fabrice Bouquet)

Examiner for Yufang Dan PhD, CITI Lyon (France), Security and self-healability enforcement of dynamic components in a service-oriented system, May 14, 2014 (Frédéric Dadeau)

Examiner for Xiaoping Che PhD, Telecom SudParis (France), Cross-Fertilizing Formal Approaches for Protocol Conformance and Performance Testing, June 26, 2014 (Frédéric Dadeau)

Examiner for Kaim Hossem PhD, LIG Grenoble (France), *Inférence automatique de modèles d'applications web et protocoles pour la détection de vulnérabilités*, December 15, 2014 (Frédéric Dadeau)

Reviewer for Valérie Murat PhD, Rennes, June 26th 2014, Tree automata extensions for the infinite states systems verification (Pierre-Cyrille Héam)

Examiner for Rafik Kheddam PhD, Valence (France), Safety software approaches for RFID systems, April 9, 2014 (Pierre-Cyrille Héam)

Examiner for Sven DeFelice PhD, Marne-la-Vallée, Codeterministic automata and acyclic automata: analysis of algorithm and random generation, July 1, 2014 (Pierre-Cyrille Héam)

Examiner for Maguy Medlej PhD, Besançon, June 30, 2014, Data Management in Periodic Wireless Sensor Networks (Olga Kouchnarenko)

Reviewer for Hikmat Farhat PhD, Toulouse, September 25, 2014, Composition of Services Behavior via Orchestrator Synthesis (Olga Kouchnarenko)

Examiner for Evelyne Contejean HDR, Orsay, June 13, 2014, Facets of Deduction (Michaël Rusinowitch)

Examiner for Myriam Paiola PhD, Paris, May 28, 2014, Verification of Security Protocols with Lists (Michaël Rusinowitch)

Examiner for Joshua Amavi PhD, Orléans, November 28, 2014, *Comparaison et évolution de schémas XML* (Michaël Rusinowitch)

Examiner for Lakhdar Akroun PhD, Clermont-Ferrand, December 8, 2014, Decidability and complexity of simulation preorder for data-centric web services (Michaël Rusinowitch)

Reviewer for Abdelkader Kersani PhD, Grenoble, October 30, 2014, *Preuves par induction dans le calcul de superposition* (Laurent Vigneron)

9.3. Popularization

Presentation of security protocols to high school teachers in Computer Science (April 17th, 2014, Véronique Cortier).

COMETE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

Note: In this section we include only the activities of the permanent internal members of Comète.

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing committee

Catuscia Palamidessi is member of:

The Executive Committee of **SIGLOG**, the ACM Special Interest Group on Logic and Computation. Since 2014.

The Organizing Committee of **LICS**, the ACM/IEEE Symposium on Logic in Computer Science. Since 2010.

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 is member of:

The steering committee of the International Workshop in Concurrency **EXPRESS**. Since 2010.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

Catuscia Palamidessi:

has served 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**.

is serving as PC chair of **LICS 2015**. 30th Annual ACM/IEEE Symposium on Logic in Computer Science. Kyoto, Japan, 6-10 July 2015.

Frank Valencia:

is serving as PC chair (with Camilo Rueda and Martin Leucker as co-chairs) of **ICTAC 2015**: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015. Co-located with **11th International Workshop on Developments in Computational Models DCM 2015**.

is serving as chair of the organising committee (with Camilo Rueda and Martin Leucker as co-chairs) of **ICTAC 2015**: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015.

8.1.2.2. Member of the conference program committee

Catuscia Palamidessi is/has been a member of the program committees of the following conferences and workshops:

ATVA 2015. The 13th International Symposium on Automated Technology for Verification and Analysis. Shanghai, China, 12-15 October 2015.

FORTE 2015. The 35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. Inria Grenoble, France, 2-4 June 2015.

TPDP 2015. Theory and Practice of Differential Privacy London, UK, 18 April 2015.

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.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

PETS 2015: The 15th Privacy Enhancing Technologies Symposium

FCS 2015: Workshop on Foundations of Computer Security

TPDP 2015: 1st workshop on the Theory and Practice of Differential Privacy

QAPL 2015: 13th Workshop on Quantitative Aspects of Programming Languages

ICISSP 2015: 1st International Conference on Information Systems Security and Privacy

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

APVP 2014: 5ème Atelier sur la Protection de la Vie Privée

Frank D. Valencia is/has been a member of the program committees of the following conferences and workshops:

PPDP 2014. The 16th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014). Canterbury, UK, September 8-10, 2014.

ICLP DC 2014. Tenth ICLP Doctoral Consortium. Vienna, Austria, July 20, 2014?

PPDP 2015. The 17th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014). Siena, Italy, July 14-16, 2015.

ICLP DC 2015. 11th ICLP Doctoral Consortium. Cork, Ireland, 31 August 2015.

8.1.2.3. Reviewer

The members of the team reviewed several papers for international conferences and workshops.

8.1.3. Journal

8.1.3.1. Member of the editorial board

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.

Member of the Editorial Board of **LIPICs: Leibniz International Proceedings in Informatics**, Schloss Dagstuhl –Leibniz Center for Informatics.

Konstantinos Chatzikokolakis is:

Editorial board member of the newly established [Proceedings on Privacy Enhancing Technologies](#) (PoPETs), a scholarly journal for timely research papers on privacy.

8.1.3.2. Reviewer

The members of the team reviewed several papers for international journals.

8.1.4. Other Editorial Activities

Catuscia Palamidessi is/has been:

Co-editor of the special issue of [Logical Methods in Computer Science](#) dedicated to selected papers of [DisCoTec 2014](#).

Co-editor (with Franck van Breughel, Elham Kashefi and Jan Rutten) of *Horizons of the Mind. A Tribute to Prakash Panangaden*. [LNCS 8464](#) Springer, 499 pages, 2014.

Co-editor (with Erika Ábrahám) of the proceedings of [FORTE 2014](#). [LNCS 8461](#) Springer, 301 pages, 2014.

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. Published on 12 December 2014.

Co-editor of the special issue of [Mathematical Structures in Computer Science](#) dedicated to the 17th International Workshop on Expressiveness in Concurrency. Published on 10 November 2014.

8.1.5. Other Activities

8.1.5.1. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

[CONCUR 2014](#) and [TGC 2014](#) (Joint keynote speaker) The 25th Conference on Concurrency Theory and the 9th International Symposium on Trustworthy Global Computing. Rome, Italy, September 2014.

[NWPT 2014](#). The 26th Nordic Workshop on Programming Theory. Halmstad, Sweden October 2014.

8.1.5.2. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the Swedish Research Council Committee for Computer Science, 2014. 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 WWTF jury – selection committee for a tenure-track position at the Faculty of Informatics at the Vienna University of Technology. Fall 2014.

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.

8.1.5.3. 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.

Frank Valencia served as:

President of the Selection Committee for the LIX Postdoctoral Fellowship. May - July 2014.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

PhD : Catuscia Palamidessi has been teaching a course for PhD students, on Quantitative Information Flow and on Differential Privacy at the department of Computer Science of the University of Pisa, Italy. April 2014. Total 20 hours.

Master : Frank D. Valencia has been teaching the masters course "Computability Theory", 60 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2014.

8.2.2. Supervision

PhD (2011-14) **Nicolás E. Bordenabe**. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2014-) **Michel Guzman**. Ecole Polytechnique. Grant Inria CORDI-S. 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.

PhD (2011-14) **Luis Fernando Pino Duque**. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

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.

8.2.3. Juries

Catuscia Palamidessi has been reviewer for the thesis of the following PhD students:

Xihui Chen (UNI-Lu, L). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Location Assurance and Privacy in Location-based Services*. Advised by Sjouke Mauw. Defended in June 2014.

Meilof Veenigen (TUE, Eindhoven, The Netherlands). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Objective Privacy – Formal analysis of data minimisation in privacy-enhancing protocols*. Advised by Sandro Etalle. Defended in June 2014.

Fabrizio Biondi (ITU, Copenhagen, Denmark). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Markovian Processes for Quantitative Information Leakage*. Advised by Andrzej Wasowski. Defended in May 2014.

Tri Mihn Ngo (University of Twente, Italy). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Qualitative and Quantitative Information Flow Analysis for Multi-threaded Programs*. Advised by University of Twente. Defended in April 2014.

Francesca Pampaloni (IMT, Lucca, Italy). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Quantitative Models of Information Flow: Tuning the Power of the Adversary*. Advised by Michele Boreale. Defended in March 2014.

Frank Valencia has been reviewer for the thesis of the following PhD students:

Laura Titolo (University of Udine, Italy). Title of the thesis: *An Abstract Interpretation Framework for Diagnosis and Verification of Timed Concurrent Constraint Languages*. Advised by Marco Comini. Defended in May 12, 2014.

8.2.4. 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.

8.3. Popularization

Catuscia Palamidessi has organized the round table “Security & Privacy : challenges of the future digital society” at the **Forum STIC**, University of Paris-Saclay, December 2014.

Konstantinos Chatzikokolakis has been one of the speakers at the above round table.

Konstantinos Chatzikokolakis has given the popularization talk “Protection de la vie privée et anonymat” at the **Journée ISN**, Académie de Créteil, March 2014.

DICE Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

Stéphane Grumbach is a member of a Scientific Committee on journalism and public welfare in the digital age at the College des Bernardins in Paris.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Stéphane Frénot, Stéphane Grumbach: Twitter, Facebook et le Web2.0, Module INSA Lyon, automne 2014

Master : Stéphane Grumbach, L'intermédiation et l'économie des ressources, cours dans le cadre du Master Biosciences, UE Sciences et Société, ENS Lyon, décembre 2014

INSA, Stéphane 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, Stéphane 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.fr> M1 (Since 2006)

INSA, Stéphane Frénot, Learn Other Languages: The aim of the course is to improve one's skills in current state-of-the-art programming and discover different ways to develop using mainly web-oriented programming languages. M1 (Since 2013)

Stéphane Grumbach, L'Economie des données, Webinaire, as part of the lecture Economie du Web, ENS Lyon, Université de Montréal, Enssib, Nov 2014

8.2.2. Supervision

Robert Riemann, decentralized voting, Sept 2014

Etienne Brodu, DataFlow compilation from JavaScript, Jan 2013

Manuel Selva, Dynamic dataflow for embedded system, Nov 2011, with Lionel Morel (Socrate Inria team)

Marie-Ange Lebre, Service oriented computing in cars, Jan 2011, with Frederic Le Mouel (Dynamid CITI team)

Rocha Goya, Smart OS for smart ambient devices, Sept 2011, with Frederic Le Mouel (Dynamid CITI team)

8.2.3. Juries

Hu Zeng, Auto-configuration, Supervision et Contrôle d'Entités Physiques par l'intermédiaire de Réseaux de Capteurs et Actionneurs, Advisor, Jan 2014

Dan Yufang, Security and self-healability enforcement of dynamic components in a service-oriented system, Advisor, may 2014

Nicolas Haderer, APISENSE : une plate-forme répartie pour la conception, le déploiement et l'exécution de campagnes de collecte de données sur des terminaux intelligents, examiner, 5 nov 2015

Jigar Solanki, Approche génerative conjointe logicielle-matérielle au développement du support protocolaire d'applications réseaux, reviewer, 27 Nov 2014

8.3. Popularization

- Stéphane Frénot and Stéphane Grumbach have been invited speakers to the BlendWebMix conference in Lyon end of October. This event of two days unites actors from different fields in the web domain, i.e. programmers, entrepreneurs, designers and scientists. Two contributions have been programmed for DICE to speak about digital and geographical territories, and about big data and intermediation platforms.
- The annual German-speaking conference DNP14 in Vienna (Austria) is a two-day event to discuss topics related to data, networks and politics and has taken place this year in September. Robert Riemann was giving a talk to introduce the concept of the C3PO project and illustrate its possibilities of application.
- Metroscope aims at being a leading Internet Observatory. It holds an annual workshop. Aurélien Faravelon presented DICE's works on intermediation at the 2014 edition.
- Séminaire Pint Of Science, Lyon, Google, Twitter, BitTorrent et BitCoin : les données, objets de toutes les convoitises <http://www.pintofscience.fr/#!lyon/ci18>, 21 Mai 2014
- Rencontres CNRS Journées citoyen CNRS, poitiers, invitation to a seminar at school about Big Data, 17-19 Oct 2014, <http://www.cnrs.fr/sciencesetcitoyens/>
- Panel Big Data, Open Data : enjeux démocratiques, colloque Le monde après Snowden, Assemblée nationale, Paris, 13-14 mars 2014
- La France dans le paysage mondial de l'intermédiation, Audition publique au Sénat, Mission commune d'information "Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet", Paris, 11 Febr 2014
- Les enjeux du numérique présentés aux députés, avec la délégation Inria, et le groupe d'études Internet et société numérique de l'Assemblée nationale, Paris, 21 janvier 2014

8.4. Invited talks

- Introduction aux algorithmes, Séminaire Journalisme et bien commun à l'heure des algorithmes, Collège des Bernardins, Paris, 16 Dec 2014
- Les données et la sécurité, Panel Les villes intelligentes, Universités de la sécurité, AN2V, Lyon, 4-5 Dec 2014
- L'intermédiation et l'économie des ressources, cours dans le cadre du Master Biosciences, UE Sciences et Société, ENS Lyon, Dec 2014
- Data is power, Panel The power of data and the internet of things, Global Forum, Geneva, 17-18 Nov 2014
- L'Economie des données, Webinaire, dans le cours Economie du Web, ENS Lyon, Université de Montréal, Enssib, Nov 2014
- "Big Data as a Resource – Political And Geopolitical Issues At Stake", Conference on Smart Data for Government, London, 23-24 Sept, 2014
- Les enjeux de l'information, Congrès de l'Union Française des Métiers de l'Événement, UNIMEV, Lille 2-4 Jul 2014
- Panel "Data Centers, Open Data, Big Data", 5th European Summit on the Future Internet, Luxembourg, 12-13 June 2014
- "The Power of Intermediation and the Geopolitical Challenge", The Diplomacy and Diversity Fellowship, a Humanity in Action program, Paris, 11 Jun 2014
- L'économie de l'intermédiation, Les grandes conférences du LIG, Grenoble, 15 May 2014

- Les données, nerf de la guerre, Journée IXXI sur la révolution numérique et la gouvernance, Lyon, 4 Apr 2014
- Les grandes plateformes de données, enjeux politiques et géopolitiques ? Institut des sciences de la communication, ISCC, Paris, 25 Mar 2014
- Panel on Big Data, Swiss STS meeting, Collecting, Organizing, Trading Big Data, University of Lausanne, 20-22 Febr 2014

PRIVATICS Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing and program committee

Claude Castelluccia : PETS' 14, WISEC 2014, AFP 2014.

Mathieu Cunche : WISEC 2014 (publicity chair).

Cédric Lauradoux : Journées C2.

Daniel Lemetayer: CPDP 2014, AFP 2014.

Marine Minier : SAR-SSI 2014

Vincent Roca : SAR-SSI 2014.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

Claude Castelluccia : WISEC 2014.

Marine Minier : CIS 2014.

8.1.2.2. Member of the conference program committee

Mathieu Cunche : WCNC 2014, APVP 2014, ICISSP 2015.

Cédric Lauradoux : Wisec 2014, SDTA 2014, CCSW 2014, Wisec 2015, Journées C2.

Vincent Roca : SPACOMM 2014, SNDS 2014

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, 80h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Signal Processing, 20h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Analysis, 20h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Introduction to Cryptography, 10h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Information Theory, 10h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Computer Architecture, 20h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Computer Security, 20h, L3, IUT-Lyon, France.

Undergraduate course : Mathieu Cunche, Introduction to computer science, 120h, L1, INSA-Lyon, France.

Undergraduate course : Cédric Lauradoux, Advanced Topics in Security, 20h, L3, ENSIMAG, France.

Master : Cédric Lauradoux, Introduction to Cryptology, 30h, M2, University of Grenoble, France.

Master : Claude Castelluccia, Advanced Topics in Security, 20h, M2, Ensimag/University of Grenoble, France.

Master : Claude Castelluccia, Advanced Topics in Security, 15h, M2, Ensimag/INPG, France.

Master : Marine Minier, Security for wireless networks, 20h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, Wireless Security, 2h, M2, INSA-Lyon, France.

8.2.2. Supervision

PhD in progress : Jagdish Acharya, 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 : 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 : 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 : Célestin Matte , Système d'observation des flux humains via Wi-Fi respectueux de la vie privée, October 2014, Marine Minier et Mathieu Cunche.

Intern (M2): Célestin Matte, Identification and Analysis of Privacy issues in the Wi-Fi technology (01/2014 - 07/2014)

Intern (M2): Pierre Brunisholz, OFDM decoding on a Virtex (02/2014- 09/2014)

Intern (M2): Emmanuel Poirier, Privacy preserving Wi-Fi tracking (02/2014-08/2014)

Intern (M1): Julia Reboul, Solving a Symmetric Key Cryptographic Problem with Constraint Programming (03/2014 - 08/2014)

Intern (M1): Pierre Rouverol, Study of Radio-Frequency tracking Technologies" (03/2014 - 08/2014)

8.2.3. Juries

HdR : Vincent Roca, Codes AL-FEC et protocoles de diffusion robuste de contenus : composants pour des services performants et passant à l'échelle, Toulouse, 19/06/2014, Claude Castelluccia.

HdR : Sebastien Gams, Respect de la vie privée dans la société de l'information, Rennes, 23/06/2014, Daniel Le Métayer.

PhD : Minh-Dung Tran, Privacy challenges in Online Targeted Advertising, Université de Grenoble, 13/11/2014, Claude Castelluccia.

PhD : Gwenaelle DEJULYS, Analysis of entropy accumulators for cryptographic RNGs, Université de Grenoble, 18/12/2014, Cédric Lauradoux.

PhD : Lukasz Olejnik, Internet Tracking and Profiling, Université de Grenoble, 30/12/2015, Claude Castelluccia.

PhD : Abdelberi Chaabane, Threats against privacy on Internet: evaluation and solutions, Université de Grenoble, 22/05/2014, Claude Castelluccia.

PhD : Ferdaouss Mattoussi, Design and optimization of AL-FEC codes: the GLDPC-Staircase codes, Université de Grenoble, 13/02/2014, Vincent Roca and Claude Castelluccia.

PhD : Guillaume Smith, Enabling Private Real-Time Applications by Exploiting the Links Between Erasure Coding and Secret Sharing Mechanisms, Université de Toulouse, 04/12/2014, Vincent Roca.

PhD : Amira Bradai, Secured trust and reputation system : analysis of malicious behaviors and optimization, Université Pierre et Marie Curie, Paris 6, 29/09/2014, Vincent Roca.

PhD : Raphaël Jamet, Protocols and Models for the Security of Wireless Ad-Hoc Networks , Université de Grenoble, 03/11/2014, Marine Minier.

8.3. Popularization

Interview of Mathieu Cunche on Radio Canada in the chronicle of Janic Tremblay, 3rd February 2014.

Interview of Mathieu Cunche on Radio France Inter in “Journal de 18h”, February 28th 2014.

Seminar of Mathieu Cunche “ Je sais tout sur vous grâce au Wi-Fi! ” Séminaire sur la Confiance Numérique at Clermont Ferrand, March 6th, 2014.

Interview of Mathieu Cunche on Radio France Info in “Tout comprendre” chronicle, March 18th, 2014.

Interview of Mathieu Cunche in Ouest-France news-paper, May 10th, 2014.

Participation of Mathieu Cunche to the TV show "Le Monde en Face" on France 5, June 17th, 2014.

Participation of Mathieu Cunche to the round table “ Numériquement vôtre ” at Futur en Seine, June 14h, 2014.

Seminar of Mathieu Cunche “ Internet: Vie privée, Surveillance et Censure ” at St-Génis Les Ollières, December 20th, 2014.

Seminar of Cédric Lauradoux “ Identifiants et guesswork ” Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux “ Identifiants et guesswork ” Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux “ Déni de Service Algorithmique ”, Journées Sécurité des Systèmes d’informations at Rouen, November 13th, 2014.

Seminar of Cédric Lauradoux “ L’Internet des Objets et l’Internet des identifiants ”, Colloque Sécurité de l’Internet des Objets (chaire de cyberdéfense et cybersécurité Saint-Cyr – Sogeti – Thalès) at Rouen, September 19th, 2014

Interview of Vincent Roca and Mathieu Cunche, “ Comment brouiller sa trace dans les réseaux ? ” Sciences et Avenir, issue 809, July 2014.

Interview of Vincent Roca, “ Spécial Grenoble : portrait de trois chercheurs ”, Le Point édition régionale, issue 2195, October 9th, 2014.

Editorial of Claude Castelluccia and Vincent Roca, “ Mobilitics Saison 2: les smartphones et leurs apps sous le microscope de la CNIL et d’Inria ”, La lettre Innovation et Prospective de la CNIL, issue 8, December 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, DAFP-RAF Inria meeting, Paris, October 16th, 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, organized by the Guilde des Utilisateurs d’Informatique Libre du Dauphiné (GUILDE), Grenoble, November 4th, 2014.

Short TV subject with Vincent Roca, “ Applications mobiles : de vrais espions ? ”, ARTE X:enius magazine, September 1st, 2014. http://www.arte.tv/guide/fr/051090-010/x-enius?vid=051090-010_PLUS7-F

Press conference, organized by CNIL in association with Inria, “ Vie privée et smartphones : les nouveaux résultats du projet Mobilitics Inria-CNIL ”, December 15th, 2014.

Seminar of Daniel Le Métayer, at the Cybersecurity Forum (ETH Zurich), 2014.

Participation of Daniel Le Métayer to a panel on privacy by design at the Annual Privacy Forum (APF 2014, Athens).

Participation of Daniel Le Métayer to Panel on at Computers Privacy and Data Protection (CPDP 2014 – Brussels).

Nomination of Daniel Le Métayer at the Commission of the French Parliament “Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l’âge du numérique.”

Organization of a seminar on privacy for the COERLE (Inria) by Claude Castelluccia and Daniel Le Métayer, November 2014.

PROSECCO Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. General chair, scientific chair

- PROSECCO organized and hosted the **The Joint EasyCrypt-F*-CryptoVerif School 2014** from Nov 24-28. The main organizers were Catalin Hritcu, Karthikeyan Bhargavan, and Pierre-Yves Strub. The school attracted over 75 participants and was primarily funded by the ERC Starting Grant CRYSP, with supporting funds from CryptoForma, MSR-Inria, and CryptoSense. The school's website is at https://wiki.inria.fr/prosecco/The_Joint_EasyCrypt-F*-CryptoVerif_School_2014
- PROSECCO hosted the **IETF TLS Working Group Interim Meeting** from October 21-22. The main organizers were Alfredo Pironti and Karthikeyan Bhargavan. The meeting involved a dozen members of industry and academia and discussed the detailed design of the next version of TLS. The meeting's website is at https://wiki.inria.fr/prosecco/IETF_TLS_Interim_October_2014

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

- ASA workshop – July 2014, Vienna, Austria: Graham Steem

8.1.2.2. Member of the conference program committee

- ETAPS HotSpot – April 2014, Grenoble, France: Bruno Blanchet
- IEEE CSF – July 2014, Vienna, Austria: Bruno Blanchet
- ACM CCS – November 2014, Scottsdale AZ, USA: Graham Steel
- ETAPS POST – April 2014, Grenoble, France: Graham Steel
- PPDP – September 2014, Canterbury, UK: Chantal Keller
- ACNS – June 2014, Lausanne, Switzerland: Catalin Hritcu
- FCS-FCC 2014 – July 2014, Vienna, Austria: Catalin Hritcu, Benjamin Smyth
- IEEE CloudCom – December 2014, Singapore: Benjamin Smyth

8.1.2.3. Reviewer

- Members of Prosecco reviewed papers for many major conferences and workshops including ACM CCS, ACM POPL, IEEE S&P, etc.

8.1.3. Journal

8.1.3.1. Member of the editorial board

Associate Editor

- of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers:
Bruno Blanchet

8.1.3.2. Reviewer

- Members of Prosecco reviewed papers for many major journals including ACM TOPLAS, ACM TISSEC, Journal of Computer Security, etc.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master: Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, universit  Paris VII, France

Doctorat: Bruno Blanchet, course on CryptoVerif, joint EasyCrypt-F*-CryptoVerif school, Paris, France

Master: Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, universit  Paris VII, France

License: Karthikeyan Bhargavan, INF431, INF421, INF672, INF321, introductory courses at at Ecole Polytechnique, Palaiseau, France

Doctorat: Catalin Hritcu, course on F*, joint EasyCrypt-F*-CryptoVerif school, Paris, France

Doctorat: Graham Steel, 3 teaching hours in Venice Ca' Foscari on Security APIs

Doctorat: Benjamin Smyth, Electronic Voting: Introduction, privacy and verifiability definitions, and examples @ CryptoBG'14, Bulgaria

8.2.2. Supervision

- PhD: Miriam Paiola
Verification of cryptographic protocols with lists of unbounded length, defended on May 28, 2014, supervised by Bruno Blanchet
- PhD in progress: Evmorfia-Iro Bartzia
Machine-checked program verification for concrete cryptography, started October 2011, supervised by Karthikeyan Bhargavan and Pierre-Yves Strub
- PhD in progress: Antoine Delignat-Lavaud
Verified security for web applications, started September 2012, supervised by Karthikeyan Bhargavan
- PhD in progress: Jean Karim Zinzindohoue
Analyzing cryptographic protocols and their implementations, started September 2014, supervised by Karthikeyan Bhargavan

8.2.3. Juries

- Cyrille Wiedling – Ph.D. – Nov. 21, 2014 – Universit  de Lorraine
Formal Verification of Advanced Families of Security Protocols: E-Voting and APIs
Bruno Blanchet (reviewer)
- Guillaume Scerri – Ph.D. – Jan. 29, 2015 – ENS Cachan
Proofs of security protocols revisited
Bruno Blanchet (reviewer)
- Bart van Delft – Licentiate – Mar. 14, 2014 – Chalmers University
Karthikeyan Bhargavan (discussion leader)

8.3. Popularization

8.3.1. Seminars

- Graham Steel: invited talks at FCS-FCC 2014 (Vienna)
- Graham Steel: invited keynote at Grande Region security day (Saarbrucken).
- Bruno Blanchet: invited talk at the Dagstuhl seminar “The synergy between programming languages and cryptography”.
- Karthikeyan Bhargavan: invited talk at the IETF TLS Working Group to discuss the Triple Handshake Attack (London)
- Karthikeyan Bhargavan: invited talk at the Dagstuhl seminar “The synergy between programming languages and cryptography”.

- Karthikeyan Bhargavan: invited talk at Les Journées Scientifiques Inria in Lille
- Karthikeyan Bhargavan: invited panelist at Security Standardization Research workshop in Surrey UK
- Karthikeyan Bhargavan: invited keynote at Santa's Crypto Workshop 2014 (Prague)
- Antoine Delignat-Lavaud: briefing at BlackHat USA on "The BEAST Wins Again: Why TLS Keeps Failing to Protect HTTP"
- Catalin Hritcu: invited keynote at Grande Region security day (Saarbrücken).
- Catalin Hritcu: seminar at Groupe de travail LTP du GDR GPL
- Catalin Hritcu: seminar at Groupe de travail Théorie des types et réalisabilité

8.3.2. Vulnerability Reports

- Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Alfredo Pironti reported the so-called Triple Handshake attacks on TLS implementations leading to security updates to all major web browsers: Google Chrome (CVE-2013-6628), Mozilla Firefox (CVE-2014-1491), Internet Explorer (CVE-2014-1771), Apple Safari (CVE-2014-1295), as well as to non-browser TLS libraries such as Oracle JSSE (CVE-2014-6457) and RSA BSAFE (CVE-2014-4630). For more details, see <http://secure-resumption.com>
- Antoine Delignat-Lavaud reported virtual host confusion attacks on a number of web servers, leading to security updates to the Akamai content delivery network, Dropbox, Bugzilla, as well as the NGINX web server. His results were presented at BlackHat USA and are summarized at <http://bh.ht.vc>
- Karthikeyan Bhargavan reported state machine attacks on major TLS libraries, such as OpenSSL (CVE-2014-3572), NSS, JSSE, CyaSSL, and SecureTransport, leading to security updates in all these libraries.