RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2016

Section Dissemination

Edition: 2017-08-25

ARIC Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Nathalie Revol, with Javier Hormigo and Stuart Oberman, were general chairs of the Arith 23 conference, Santa Clara, California, USA.

9.1.1.2. Member of the Organizing Committees

Nathalie Revol was the organizer of the SWIM 2016: Summer Workshop on Interval Methods, gathering above 35 participants in Lyon, June 2016.

Bruno Salvy was a co-organizer of the meeting Alea'16 gathering about 80 participants in Luminy, March 2016.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Jean-Michel Muller belongs to the 3-member board of the steering committee of the Arith series of conferences.

9.1.2.2. Member of the Conference Program Committees

Nathalie Revol was a member of the program committees of REC'16 and SCAN 2016.

Bruno Salvy was a member of the program committee of AofA'16, Krakow, Poland.

Damien Stehlé was member of the program committees of Asiacrypt'16, Eurocrypt'17, SCN'16, ANTS'16, PKC'16 and PQCrypto'16.

Benoît Libert was member of the program committees of PKC'16, Africacrypt'16, ACM-CCS 2016, Eurocrypt'17.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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*.

Nathalie Revol is a member of the editorial board of the journal *Reliable Computing*.

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 collection *Texts and Monographs in Symbolic Computation* (Springer).

Gilles Villard is a member of the editorial board of the *Journal of Symbolic Computation*.

9.1.4. Invited Talks

Damien Stehlé gave an invited talk at the YACC conference (Porquerolles, June), on the Learning With Errors Problem. He gave an invited talk at the HEAT workshop (Paris, July) on lattice reduction.

Jean-Michel Muller gave an invited talk at a minisymposium on reproducible research at the CANUM conference (Obernai, May).

Claude-Pierre Jeannerod and Clément Pernet gave invited talks at RAIM (Rencontres Arithmétique de l'Informatique Mathématique; Banyuls-sur-mer, June).

Nathalie Revol gave an invited talk at a minisymposium on numerical reproducibility for high-performance computing at SIAM Parallel Processing (Paris, April).

9.1.5. Leadership within the Scientific Community

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).

Paola Boito and Claude-Pierre Jeannerod are members of the scientific committee of JNCF (Journées Nationales de Calcul Formel).

Nathalie Revol is the chair of the IEEE 1788 group for the standardization of interval arithmetic: the work now addresses the set-based model and its implementation using simple IEEE-754 formats (IEEE P1788.1).

9.1.6. Scientific Expertise

Jean-Michel Muller is a member of the Scientific Council of CERFACS (Toulouse). He was a member of the Scientific Council of the "La Recherche" prize for 2015.

Jean-Michel Muller is a member of the steering committee of the "Defi 7" (information sciences) of the French Agence Nationale de la Recherche (ANR).

Bruno Salvy was a member of the recruitment committees for University Professors in Bordeaux (computer science) and in Toulouse (Mathematics).

Damien Stehlé is a member of the 2016 Gilles Kahn PhD award committees for 2016.

Claude-Pierre Jeannerod was a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble Rhône-Alpes.

9.1.7. Research Administration

Guillaume Hanrot is director of the LIP laboratory (Laboratoire de l'Informatique du Parallélisme).

Jean-Michel Muller is co-director of the Groupement de Recherche (GDR) *Informatique Mathématique* of CNRS.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Claude-Pierre Jeannerod, 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* (12h), M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

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

Master: Damien Stehlé, Cryptography, 12h, ENS de Lyon.

Master: Benoît Libert, Computer science and privacy, 12h, ENS de Lyon; Cryptography, 12h, ENS de Lyon.

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

Master: Bruno Salvy, Calcul Formel (9h), MPRI.

Master: Bruno Salvy, Mathématiques expérimentales (44h), École polytechnique.

Master: Bruno Salvy, Logique et complexité (32h), École polytechnique.

9.2.2. Supervision

- PhD: Serge Torres, *Tools for the design of reliable and efficient function evaluation libraries*, École normale supérieure de Lyon; defended on September 22, 2016; co-supervised by Nicolas Brisebarre and Jean-Michel Muller.
- PhD: Vincent Neiger, *Bases of relations in one or several variables: fast algorithms and applications*, École normale supérieure de Lyon; defended on November 30, 2016; co-supervised by Claude-Pierre Jeannerod and Gilles Villard (together with Éric Schost (U. Waterloo, Canada)).
- PhD: Silviu-Ioan Filip, *Robust tools for weighted Chebyshev approximation and applications to digital filter design*, École normale supérieure de Lyon; defended on December 7, 2016; co-supervised by Nicolas Brisebarre and Guillaume Hanrot.
- 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: Louis Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, since September 2013, co-supervised by Alin Bostan (SpecFun team) and Bruno Salvy.
- PhD in progress: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, since September 2014, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.
- PhD in progress: Fabrice Mouhartem, *Privacy-preserving protocols from lattices and bilinear maps*, since September 2015, supervised by Benoît Libert.
- PhD in progress: Chen Qiang, *Applications of Malleability in Cryptography*, since September 2016, co-supervised by Benoît Libert, Adeline Langlois (IRISA) and Pierre-Alain Fouque (IRISA).
- PhD in progress: Weiqiang Wen, *Hard problems on lattices*, since September 2015, supervised by Damien Stehlé.
- PhD in progress: Alice Pellet–Mary, *Cryptographic obfuscation*, since September 2016, supervised by Damien Stehlé.
- PhD in progress: Florent Bréhard, *Outils pour un calcul certifié. Applications aux systèmes dynamiques et à la théorie du contrôle*, since September 2016, co-supervised by Nicolas Brisebarre, Mioara Joldeş (LAAS, Toulouse) and Damien Pous (LIP).

9.2.3. Juries

Paola Boito was an external reviewer for the PhD thesis of Bahar Arslan (University of Manchester, UK). She was also in the PhD committee of Louis Dumont (LIX, École polytechnique).

Claude-Pierre Jeannerod was in the PhD committee of Alexandre Temperville (CRIStAL, U. Lille 1).

Fabien Laguillaumie was a reviewer for the Habilitation thesis of Abderrahmane Nitaj (LMNO, U. Caen) and for the PhD thesis of Mario Cornejo-Ramirez (LIENS, UPSL).

Jean-Michel Muller was a reviewer for the PhD thesis of Arjun Suresh (U. Rennes). He was in the Habilitation committee of Claude Michel (U. Nice Sophia Antipolis).

Nathalie Revol was in the PhD committee of Rafife Nheili (U. Perpignan Via Domitia).

Bruno Salvy was a reviewer for the PhD thesis of Thibaut Verron (LIP6, UPMC) and for the HdR of Loïck Lhôte (Greyc, U. Caen). He was also in the PhD committees of Wenjie Fang (LIAFA, U. Paris-Diderot) and Louis Dumont (LIX, École polytechnique).

Damien Stehlé was a reviewer for the PhD thesis of Hansol Ryu (SNU, South Korea). He was in the PhD committee of Thijs Laarhoven (TU Eindhoven, The Netherlands) and in the Habilitation committee of Hoeteck Wee (DI, CNRS).

9.3. Popularization

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

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

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

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

AROMATH Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Member of the Organizing Committees

Laurent Busé was the main organizor of the BIRS-CMO conference "*Computational Algebra and Geometric Modeling*" that took place at Oaxaca, Mexico, August 7-12 2016. He also co-organized with A. Dimca (Univ. Nice) a mini-workshop "*commutative algebra and applications*" that took place at the laboratory of mathematics of the university of Nice, September 22-23. He also co-organized a *week of studies maths-industry* (SEME) that took place at the CRI-SAM January 25-29.

Evelyne Hubert was part of the organizing committee of the collaborative research workshop *Women in Shape: Modeling Boundaries of Objects in 2- and 3-Dimensions* that took place June 6-12 at the Nesin Mathematics Village in Turkey.

8.1.2. Scientific Events Selection

8.1.2.1. Reviewer

Laurent Busé, Evelyne Hubert and Bernard Mourrain reviewed submissions for the conference ISSAC'16.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

Bernard Mourrain is associate editor of the Journal of Symbolic Computation (since 2007) and of the SIAM Journal on Applied Algebra and Geometry (since 2016).

Ioannis Emiris is associate editor of the Journal of Symbolic Computation (since 2003) and of Mathematics in Computer Science (since 2016).

Evelyne Hubert is associate editor of the Journal of Symbolic Computation (since 2007) and became a reviewer for Mathematical Reviews (MathSciNet) this year.

8.1.3.2. Reviewer - Reviewing Activities

Laurent Busé wrote reviews for the following international journals: Journal of Symbolic Computation, Journal of Algebra, Computer Aided Geometric Design, Mathematical and Computational Applications, Graphical Models, Linear Algebra and its Applications, SIAM Journal on Applied Algebra and Geometry, Transactions on Graphics, the Quarterly Journal of Mathematics and Math. Zeitschrift. He also wrote reviews for the ISSAC 2016 and the Eurographics 2017 international conferences.

Evelyne Hubert reviewed for the journal *Mathematics of Computation*, the *Journal of Symbolic Computation*, the *Journal of Pure & Applied Algebra*, the journal *Mathematics in Computer Science*, and Springer book series *Texts and Monographs in Symbolic Computation*,

Bernard Mourrain reviewed for the journal *Advances in Computational Mathematics*, the *Journal of Algebra and Applications*, the journal *Collectanea Mathematica*, the journal *Computer Aided Design*, the journal *Computer Aided Geometric Design*, the journal *Foundations of Computational Mathematics*, the *Journal of Pure and Applied Algebra*, the journal *SIAM Journal on Optimization*, the *Transactions on Mathematical Softwares*.

8.1.4. Invited Talks

Laurent Busé was invited to give a talk at the Inria project-team ARIC seminar, May 26, at the conference "Computational Algebra, Algebraic Geometry and Applications", in honor of Alicia Dickenstein, that took place at Buenos Aires, Argentina, August 1-3 2016, at the *H2020 day* organized at the CRI-SAM to give a testimony on the writing of the successful MCA-ITN proposal ARCADES.

Ioannis Emiris gave an invited talk at ACM International Symposium on Symbolic & Algebraic Computation, Waterloo, Canada, July 2016.

Evelyne Hubert was invited to give a talk at the *Computational Mathematics Colloquium* at University of Waterloo, Canada (January 2016); at the workshop on *Théorie Effective des Invariants*, at the Insitut de Mathématiques de Marseille (June 2016); at the workshop on *Symmetry, Invariants, Reduction* in RWTH Aachen University (September 2016); at the BIRS-CMO conference *Sparse Interpolation, Rational Approximation and Exponential Analysis* in Oaxaca, Mexico (November 2016). She was also invited (and supported) to partitipate to the American Institute of Mathematics workshop *Algebraic Vision* in San Jose, California (May 2016); and the BIRS-CMO conference *Computational Algebra and Geometric Modeling* in Oaxaca, Mexico (August 2016); and to the CIRM conference *Multivariate Approximation and Interpolation with Applications* where she presented a poster (September 2016).

Bernard Mourrain was invited to give a talk at the MFO workshop *Mathematical Foundations of Isogeometric Analysis* Oberwolfach, Germany (February 2016), at the conference "Computational Algebra, Algebraic Geometry and Applications", in honor of Alicia Dickenstein, that took place at Buenos Aires, Argentina, August 1-3 2016, at the BIRS-CMO conference *Computational Algebra and Geometric Modeling* in Oaxaca, Mexico (August 2016), at the CIRM conference *Multivariate Approximation and Interpolation with Applications* Marseille, France (September 2016), at the BIRS-CMO conference *Sparse Interpolation, Rational Approximation and Exponential Analysis* in Oaxaca, Mexico (November 2016).

8.1.5. Leadership within the Scientific Community

Evelyne Hubert, in collaboration with Géraldine Morin, lead a collaborative research group at the workshop *Women in Shape: Modeling Boundaries of Objects in 2- and 3-Dimensions*.

8.1.6. Scientific Expertise

Bernard Mourrain was member of the committee of the HCERES for the evaluation of IRMAR, University of Rennes.

Evelyne Hubert was a member of the admissibility jury for the *Chargé de Recherche* position in CRI-Rennes Bretagne Atlantique.

Laurent Busé was a member of the CRI-SAM committee "Actions Marquantes", March 25. He is also a board member of the (national) labex AMIES (CRI-SAM representative) and a member of the steering committee of the MSI, *Maison de la Modélisation, de la Simulation et des Interactions* of the University Côte d'Azur.

8.1.7. Research Administration

Evelyne Hubert is an elected member of the Inria national *Commission d'Evaluation*.

Laurent Busé is an elected member of the CPRH (Commission Permanente de Ressources Humaines) of the math laboratory of the university of Nice. He was also appointed Inria representative at the "Academic Council" and the "Research Commission" of the university of Nice.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Ioannis Emiris, Discrete Math, 53, L1, NKU Athens, Greece.

Licence : Ioannis Emiris, Soft development for algorithmic problems, 53, L3, NKU Athens, Greece

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

Master : Laurent Busé, Geometric Modeling, 27h ETD, M2, EPU of the university of Nice-Sophia Antipolis.

8.2.2. Supervision

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: Ahmed Blidia, New geometric models for the design and computation of complex shapes. ARCADES Marie Skłodowska-Curie ITN, started in September 2016, supervised by Bernard Mourrain.

PhD in progress: Jouhayna Harmouch, Low rank structured matrix decomposition and completion. Cotutelle Univ. Liban, started in November 2015, cosupervised by Houssam Khalil and Bernard Mourrain.

PhD in progress: Anna Karasoulou, Exploiting structure in polynomial systems. Excellence awards (Greece), started in November 2011, supervised by Ioannis Emiris.

PhD in progress: Ioannis Psarros, Geometric approximation algorithms. Thales network (Greece), started in May 2015, supervised by Ioannis Emiris.

PhD in progress: Evangelos Bartzos, Modeling motion. ARCADES Marie Skłodowska-Curie ITN, started in May 2016, supervised by Ioannis Emiris.

PhD in progress: Evangelos Anagnostopoulos, Geometric algorithms for massive datasets. Started in May 2016, supervised by Ioannis Emiris.

PhD in progress: Clement Laroche, Change of representation in CAGD. ARCADES Marie Skłodowska-Curie ITN, started in Nov. 2016, supervised by Ioannis Emiris.

PhD in progress: Alvaro-Javier Fuentes-Suarez, Skeleton-based modeling of smooth shapes. ARCADES Marie Skłodowska-Curie ITN, started in October 2016, supervised by Evelyne Hubert.

Master in Computer Science: Paul Görlach, University of Bonn. Rotational invariants of ternary quartics. CRI-SAM tranverse action AROMATH-ATHENA. August-December 2016, supervised by Evelyne Hubert.

PhD in progress: Fatmanur Yildirim, Distances between points, rational Bézier curves and surfaces by means of matrix-based implicit representations. ARCADES Marie Skłodowska-Curie ITN, started in October 2016, supervised by Laurent Busé.

8.2.3. Juries

Evelyne Hubert was a referee for the PhD of Louis Dumont entitled *Algorithmes rapides pour le calcul symbolique de certaines intégrales de contour à paramètre*, Université Paris-Saclay, École Polytechnique, Inria Saclay Île-de-France.

Bernard Mourrain was a referee for the PhD of Emil Horobet, entitled *Tensors of low rank*, Univ. of Technology, Eindhoven, Netherland.

Laurent Busé was a referee for the PhD of Thibaut Verron entitled *Régularisation du calcul de bases de Gröbner pour des systèmes avec poids et déterminantiels, et application en imagerie médicale*, Université Pierre et Marie Curie, Paris, France, September 26.

CARAMBA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organization

10.1.1.1. Member of the Organizing Committees

- Together with Anne-Lise Charbonnier (Inria Nancy – Grand Est), the Caramba team is organizing the "Journées Codage et Cryptographie 2017", whose objective is to regroup the French speaking community working on error-correcting codes and on cryptography. It is affiliated with the "Groupe de travail C2" of the GDR-IM.

10.1.2. Scientific Events Selection

10.1.2.1. Member of steering committees

- Pierrick Gaudry is a member of the steering committee of the Workshop on Elliptic Curve Cryptography (ECC).

10.1.2.2. Member of the Conference Program Committees

- Emmanuel Thomé was a member of the program committee of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2016).
- Marine Minier was a member of the Program Committee of the conference MyCrypt 2016.
- Pierrick Gaudry was a member of the Program Committee of the conference Selected Areas in Cryptography SAC 2016 and of EUROCRYPT 2017.
- Paul Zimmermann was a member of the Program Committee of the International Workshop on the Arithmetic of Finite Fields (WAIFI 2016).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Pierrick Gaudry is a member of the editorial board of the journal Applicable Algebra in Engineering, Communication and Computing.

10.1.3.2. Reviewer - Reviewing Activities

Members of the project-team did share in reviewing submissions to renowned conferences and journals. Actual publications venues are not disclosed for anonymity reasons.

10.1.4. Invited Talks

- Emmanuel Thomé was invited as a Distinguished Lecturer for the Computer and Information Security Seminar at the University of Pennsylvania in November 2016.
- Pierrick Gaudry was invited speaker at the YACC 2016 conference in Porquerolles, at the workshop "Mathematical Structures for Cryptography" in Leiden (Netherlands), and at the "Journées Aléa 2016" in Marseille.

10.1.5. Other committees

- Jérémie Detrey is chairing the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) of the Inria Nancy – Grand Est research center.
- Emmanuel Thomé is a member of
  - the management committee for the research project "CPER Cyberentreprises" (co-chair).

  - the *Comité Local Hygiène, Sécurité, et Conditions de Travail* of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
- Pierre-Jean Spaenlehauer is a member of the *Commission développement technologique* (CDT) of the Inria Nancy – Grand Est research center.
- Paul Zimmermann is member of the Scientific Committee of the EXPLOR *Mésocentre*, and was member until August of the Inria Evaluation Board and the CoSI (*Commission Scientifique*).

10.1.6. Research Administration

- Laurent Grémy is a member of the *Conseil de laboratoire* of the Loria.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Jérémie Detrey, *Sécurité des systèmes d'information*, 6 hours (practical sessions), M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Master: Pierre-Jean Spaenlehauer, *Introduction à la cryptographie*, 18h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Master: Pierre-Jean Spaenlehauer, *Introduction à la sécurité des systèmes et à la cryptographie*, 32h eq. TD, M2 Mathématiques IMOI, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Master: Emmanuel Thomé, *Introduction to Cryptography*, 12 hours (lectures), M1, Télécom Nancy, Villers-lès-Nancy, France.

Master: Emmanuel Thomé, *Cryptography and Security*, 20 hours (lectures + exercises), M2, Télécom Nancy and École des Mines de Nancy, France.

Licence: Jérémie Detrey, *Méthodologie*, 24 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Licence: Jérémie Detrey, *Sécurité des applications Web*, 2 hours (lecture), L1, Université de Lorraine, IUT Charlemagne, Nancy, France.

Jérémie Detrey, *Introduction à la sécurité et à la cryptographie*, 10 hours (lectures) + 10 hours (tutorial sessions) + 10 hours (practical sessions), L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Licence: Pierrick Gaudry, *Méthodologie*, 48 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

10.2.2. Supervision

Internship: Nicolas Levy, *Algorithmes de factorisation d'entiers basés sur la structure des corps quadratiques réels*, L3 ÉNS Lyon, June-July, Pierre-Jean Spaenlehauer.

Internship: Joshua Peigner, *Factorisation d'idéaux pour l'implantation du crible algébrique*, ÉNS Rennes, June-July, Emmanuel Thomé.

Internship: Robin Fedele, *Consolidation de la couche Python de CADO-NFS*, Univ. Lorraine, May-June, Paul Zimmermann.

Internship: Élise Tasso, *Étude comparative de divers algorithmes de friabilisation*, Mines Nancy, October-June (1 day each week), Pierrick Gaudry.

Ph.D. in progress: Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, Univ. Lorraine; since Sep. 2015, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

Ph.D. in progress: Svyatoslav Covanov, *Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides*, since Sep. 2014, Jérémie Detrey et Emmanuel Thomé.

Ph.D. in progress: Laurent Grémy, *Analyse et optimisation d'algorithmes de cribles arithmétiques*, since Oct. 2013, Pierrick Gaudry & Marion Videau.

Ph.D. defended: Hugo Labrande, *Explicit computation of the Abel-Jacobi map and its inverse* [1], defended on November 14th, 2016.

10.2.3. Juries

Marine Minier: reviewer of the PhD *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs* by Tania Richmont defended at Univ. Jean Monnet Saint-Etienne, October 24th, 2016.

Pierrick Gaudry: reviewer of the PhD *Computational Aspects of Jacobians of Hyperelliptic Curves* by Alina Dudeanu defended at EPFL, Switzerland; member of the jury for the PhD of Florent Ulpat Rovetta (Marseille) and of Hugo Labrande (Nancy).

Emmanuel Thomé: reviewer (and president of jury) of the Habilitation Thesis *Contributions à la Résolution Algébrique et Applications en Cryptologie* by Guénaël Renault, defended at University Pierre et Marie Curie, December 8th, 2016.

Emmanuel Thomé: jury member (advisor) for the PhD of Hugo Labrande (see above).

10.3. Popularization

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

CASCADE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Events and Activities

- a regular seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html
- quarterly Paris Crypto Days (https://pariscryptoday.github.io) supported by CryptoCloud and aSCEND
- working group on lattices (http://perso.ens-lyon.fr/damien.stehle/LATTICE_MEETINGS.html), joint with ENS Lyon
- BibTeX database of papers related to Cryptography, open and widely used by the community (https://cryptobib.di.ens.fr)

8.1.1.2. Steering Committees of International Conferences

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

8.1.1.3. Other Steering Committees

- steering committee of the Coding and Cryptography working group (GT-C2 - https://crypto.di.ens.fr/c2:main) of the *Groupe de Recherche Informatique Mathématique* (GDR-IM): Damien Vergnaud is the Head of this steering committee

8.1.1.4. Board of International Organisations

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2018), David Pointcheval (2008–2016)

8.1.2. Scientific Events Selection

8.1.2.1. Program Committee Chair

- Africacrypt '16 – 13-15 April (Fes, Morocco): David Pointcheval

8.1.2.2. Program Committee Member

- Financial Crypto '16 – 22–26 February (Barbados): Damien Vergnaud
- PKC '16 – 6-9 March (Taiwan): David Pointcheval
- Africacrypt '16 – 13-15 April (Fes, Morocco): Georg Fuchsbauer
- Eurocrypt '16 – 8-12 May (Vienna, Austria): Michel Abdalla and Georg Fuchsbauer
- AsiaPKC 2016 – 30 May 30 - 03 June (Xi'an, China): Damien Vergnaud
- Crypto '16 – 14-18 August (Santa Barbara, California, USA): David Pointcheval
- ACM CCS '16 – 24-28 October (Vienna, Austria): Hoeteck Wee
- ProvSec '16 – 10-12 November (Nanjing, China): Georg Fuchsbauer
- CANS '16 – 14-16 November (Milan, Italy): Georg Fuchsbauer
- Asiacrypt '16 – 4-8 December (Hanoi, Vietnam): Georg Fuchsbauer

8.1.3. Editorial Boards of Journals

Editor-in-Chief

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

Associate Editor

– of *IET Information Security*: Michel Abdalla
– of *ETRI Journal*: Michel Abdalla
– of *Applicable Algebra in Engineering, Communication and Computing*: David Pointcheval

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Master: David Pointcheval, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS
- Master: Michel Abdalla, David Pointcheval, Cryptography, M2, MPRI
- Master: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: David Pointcheval, Cryptography, M2, ESIEA
- IACR-SEAMS School on "Cryptography: Foundations and New Directions": David Pointcheval

8.2.2. Defenses

- PhD: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, ENS, December 12th, 2016 (Supervisor: Damien Vergnaud)
- PhD: Alain Passelègue, Algebraic Frameworks for Pseudorandom Functions, ENS, December 9th, 2016 (Supervisor: Michel Abdalla)
- PhD: Mario Cornejo, Security for the cloud, ENS, November 17th, 2016 (Supervisor: Michel Abdalla)
- HdR: Hoeteck Wee, Advances in Functional Encryption, ENS, July 1st, 2016
- PhD: Fabrice Ben Hamouda, Diverse Modules and Zero-Knowledge, ENS, July 1st, 2016 (Supervisors: Michel Abdalla & David Pointcheval)

8.2.3. Supervision

- PhD in progress: Raphael Bost, Symmetric Searchable Encryption, from 2014, David Pointcheval (with Pierre-Alain Fouque, at Rennes)
- 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: Pierrick Meaux, Lattice-Based Cryptography – Advanced Features, from 2014, Vadim Lyubashevsky
- PhD in progress: Thierry Mefenza Nountu, Number-Theoretic Study of Pseudorandom Cryptographic Primitives, from 2014, Damien Vergnaud
- PhD in progress: Aurélien Dupin, Multi-Party Computations, from 2015, David Pointcheval (with Christophe Bidan, at Rennes)
- PhD in progress: Pierre-Alain Dupont, Secure Communications, from 2015, David Pointcheval
- PhD in progress: Romain Gay, Functional Encryption, from 2015, Michel Abdalla & Hoeteck Wee

- PhD in progress: Dahmun Gourdazi, Secure and Fast Cryptographic Implementation for Embedded Devices, from 2015, Damien Vergnaud
- PhD in progress: Louiza Khati, Disk Encryption Modes, from 2015, Damien Vergnaud
- PhD in progress: Michele Minelli, Increased efficiency and functionality through lattice-based cryptography, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Anca Nitulescu, Verifiable Outsourced Computations, from 2015, David Pointcheval
- PhD in progress: Razvan Rosie, Practical Functional Encryption Schemes For the Cloud, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Quentin Santos, Advanced Cryptography from a Blockchain, from 2015, David Pointcheval
- PhD in progress: Jérémy Chotard, Attribute-Based Encryption, from 2016, David Pointcheval (with Duong Hieu Phan, at Limoges)
- PhD in progress: Michele Orrù, Functional Encryption, from 2016, Hoeteck Wee & Georg Fuchsbauer

8.2.4. Juries

- PhD Adrian Thillard. *Countermeasures to side-channel attacks and secure multi-party computation* – ENS – France, December 12th, 2016: Damien Vergnaud (supervisor)
- PhD Alain Passelègue. *Algebraic Frameworks for Pseudorandom Functions* – ENS – France, December 9th, 2016: Michel Abdalla (supervisor)
- PhD Mario Cornejo. *Security for the cloud* – ENS – France, November 17th, 2016: Michel Abdalla (supervisor), David Pointcheval
- PhD Christian Janson. *On the Verification of Computation and Data Retrievability* – Royal Holloway University of London – UK, October 11th, 2016: Michel Abdalla
- PhD Brice Minaud. *Analyse de primitives cryptographiques récentes* – Université Rennes I – France, October 7th, 2016: David Pointcheval
- PhD Houda Ferradi. *Integrity, Authentication and Confidentiality in Public-Key Cryptography* – ENS – France, September 22nd, 2016: Michel Abdalla
- HdR Hoeteck Wee. *Advances in Functional Encryption* – ENS – France, July 1st, 2016: Michel Abdalla, David Pointcheval
- PhD Fabrice Ben Hamouda. *Diverse Modules and Zero-Knowledge* – ENS – France, July 1st, 2016: Michel Abdalla & David Pointcheval (supervisors)
- PhD Alberto Battistello. *On the security of embedded systems against physical attacks* – UVSQ – France, June 29th, 2016: David Pointcheval
- PhD Antoine Delignat-Lavaud. *On the Security of Authentication Protocol for the Web* – ENS – France, March 14th, 2016: David Pointcheval
- PhD Rémy Chrétien. *Automated analysis of equivalence properties for cryptographic protocols* – ENS Cachan – January 11th, 2016: David Pointcheval

DATASHAPE Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Jean-Daniel Boissonnat and Frédéric Chazal co-organized the joint GUDHI-TOPDATA workshop in Porquerolles, October 17-20.

Frédéric Chazal co-organized the SMAI-SIGMA Conference 2016 at Luminy (CIRM) in November.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Maks Ovsjanikov: Paper co-chair of the Symposium on Geometry Processing 2016 (SGP 2016).

10.1.2.2. Member of the Conference Program Committees

Frédéric Chazal: Symposium on Geometry Processing 2016 (SGP 2016).

Steve Oudot: Symposium on Geometry Processing 2016 (SGP 2016).

Marc Glisse: Symposium on Computational Geometry (SoCG 2016).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

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

Frédéric Chazal is a member of the Editorial Board of *SIAM Journal on Imaging Sciences*, *Discrete and Computational Geometry (Springer)*, *Graphical Models (Elsevier), and Journal of Applied and Computational Topology (Springer)*.

Steve Oudot is a member of the Editorial Board of *Journal of Computational Geometry*.

10.1.4. Invited Talks

Frédéric Chazal, ACCAPT conference, Aalborg, Danmark, April 2016.

Frédéric Chazal, Joint Mathematical Meetings, Seattle, USA, January 2016.

Frédéric Chazal, Séminaire Parisien de Géométrie Algorithmique, Paris, October 2016.

Frédéric Chazal, 9th International Conference of theERCIM WG on Computational and Methodological Statistics, December 2016.

Steve Oudot, ACCAPT conference, Aalborg, Danmark, April 2016.

Steve Oudot, Workshop SIGMA 2016, CIRM, France, November 2016.

Steve Oudot, Applied Topology Seminar, Brown University, USA, November 2016.

Steve Oudot, Topology and Neuroscience Seminar, Princeton University, USA, November 2016.

10.1.5. Scientific Expertise

Frédéric Chazal was a member of the ANR committee, CES 40 (Mathematics and Computer Science).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master : Frédéric Chazal, Analyse Topologique des Données, 30h eq-TD, Université Paris-Sud, France.

Master : Jean-Daniel Boissonnat and Marc Glisse, Computational Geometry Learning, 36h eq-TD, M2, MPRI, France.

Doctorat : Frédéric Chazal and Bertrand Michel, An introduction to Topological Data Analysis, 18h eq-TD, Universitad Autonoma de Barcelona, Spain.

Master : Steve Oudot, Topological Data Analysis, 45h eq-TD, M1, École Polytechnique, France.

Master : Steve Oudot and Frédéric Cazals, Geometric Methods for Data Analysis, 30h eq-TD, M1, École Centrale Paris, France.

Master : Jean-Daniel Boissonnat, Winter School on Computational geometry and Topology, Inria Sophia Antipolis Méditerrannée, January 2016.

Doctorat : Steve Oudot, École Mathématique en Afrique on *Topologie différentielle, géométrie algébrique et applications*, La Marsa, Tunisia, March-April 2016.

Doctorat : Steve Oudot, Summer School on Mathematical Methods for High-Dimensional Data Analysis, Technical University of Munich, Germany, July 2016.

10.2.2. Supervision

PhD: Thomas Bonis, Statistical Learning Algorithms for Geometric and Topological Data Analysis, December 1st, 2016, Frédéric Chazal.

PhD : Mael Rouxel-Labbé, Génération de maillages anisotropes, december 16, 2016, Jean-Daniel Boissonnat.

PhD: Ruqi Huang, Algorithms for topological inference in metric spaces, December 14, 2016, Frédéric Chazal.

PhD in progress: Eddie Aamari, A Statistical Approach of Topological Data Analysis, started September 1st, 2014, Frédéric Chazal (co-advised by Pascal Massart).

PhD in progress: Claire Brécheteau, Statistical aspects of distance-like functions , started September 1st, 2015, Frédéric Chazal (co-advised by Pascal Massart).

PhD in progress: Bertrand Beaufils, Méthodes topologiques et apprentissage statistique pour l'actimétrie du piéton à partir de données de mouvement, started November 2016, Frédéric Chazal (co-advised by Bertrand Michel).

PhD in progress: Mathieu Carrière, Topological signatures for geometric data, started November 1st, 2014, Steve Oudot.

PhD in progress: Jérémy Cochoy, Decomposition and stability of multidimensional persistence modules, started September 1st, 2015, Steve Oudot.

PhD in progress: Nicolas Berkouk, Categorification of topological graph structures, started November 1st, 2016, Steve Oudot.

PhD in progress: Alba Chiara de Vitis, Concentration of measure and clustering.

PhD in progress: Siargey Kachanovich, Approximate algorithms in higher dimensional geometry.

PhD in progress: François Godi, Data structures and algorithms for topological data analysis and high dimensional geometry.

10.2.3. Juries

Frédéric Chazal was a member (and reviewer) of the PhD defense committee of Mariia Fodetenkova (Inria Nancy).

GRACE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- D. Augot is member of the committee of the CCA seminar on coding and cryptology. This seminar regularly attracts around 30 participants.

10.1.2. Scientific Events Selection

10.1.2.1. Reviewer

- D. Augot was reviewer for International Symposium on Information Theory

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- 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.
- F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.
- A. Couvreur was editor with Alp Bassa (Bogazici University, Turkey) and David Kohel (Aix-Marseille University) of a number of *AMS Contemporary Mathematics* for the proceedings of the conference AGCT (*Arithmetic Geometry Cryptography and Coding Theory*) 2015.

10.1.3.2. Reviewer - Reviewing Activities

- D. Augot was reviewer for
  - Discrete Mathematics
  - Designs, Codes and Cryptography
  - Linear and Multilinear Algebra
  - Finite Fields and their applications
- A. Couvreur was reviewer for
  - Discrete Mathematics
  - Designs, Codes and Cryptography
  - Journal of Algebra

10.1.4. Invited Talks

- D. Augot was invited speaker at Yet Another Cryptography Conference (YACC), Porquerolles, June 2016.
- B. Smith was an invited speaker at the 20th international Workshop on Elliptic Curve Cryptography (ECC), Izmir, Turkey, September 2016.
- A. Couvreur gave a talk to represent the group *Codes et Cryptographie* of the GdR *Informatique Mathématiques* (GdR IM) at the *Journées nationales du GdR IM* at University Paris 13 (January 13).

10.1.5. Scientific Expertise

- D. Augot participated in a round table at a workshop organized by French National Assembly (lower house) at, on blockchains (March 24th).
- D. Augot participated in a round table at Paris Dauphine on blockchains, organized by the chair "Chaire Gouvernance & Régulation" (November 1).
- D. Augot made a talk on hashing and blockchain at a workshop on blockchains held at Institut Poincaré (November 16).

10.1.6. Teaching in international postgraduate summer schools

- B. Smith gave lectures on *Basic public-key constructions with elliptic curves* and *Advanced constructions in curve-based cryptography* at the *Summer school on real-world crypto and privacy*, Sibenik, Croatia, June 2016.
- B. Smith gave a course on *asymmetric cryptography and elliptic curves* at the *Crypto-CO summer school on cryptography and security*, Bogota, Colombia, July 2016.
- B. Smith gave lectures on elliptic curves at the *ECC2016 Computational Algebraic Number Theory School*, Izmir, Turkey, September 2016.

10.1.7. Research Administration

Committees

- A. Couvreur is an elected member of Saclay's *comité de centre*.
- A. Couvreur is an elected member of Saclay's *Comité local Hygiène, Sécurité et Conditions de Travail*.
- A. Couvreur is the *jeune chercheur référent* for the *commission de suivi doctoral* of Inria Saclay.
- D. Augot is a member of LIX's *conseil de direction*.
- D. Augot is the vice-head of Inria's *comité de suivi doctoral*
- D. Augot is a member of LIX's *assemblée des chefs d'équipe*
- D. Augot is elected member of the *conseil académique consultatif* of Paris-Saclay University.
- F. Levy-dit-Vehelis a representative of "enseignants-chercheurs" of LIX.
- F. Morain, B. Smith and A. Couvreur 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*.
- F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).
- 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.
- B. Smith is the academic coordinator for Computer Science in the new *Bachelor* program at École polytechnique.

Committees

- D. Augot was in the committee assessing candidates for Univ. Paris 8.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence :

- D. Augot was mentoring a group of polytechnique students on a L3 projet on homomorphic encryption and voting (6 students)
- D. Augot was mentoring a group of polytechnique students on a L3 projet on blockchains and hyperledger, in collaboration with Orange (5 students)
- F. Levy-dit-Vehel, “Mathématiques discrètes pour la protection de l’information”, 24h (equiv TD), 2nd year (L3), ENSTA ParisTech, France.
- J. Lavauzelle, 1I002, “Introduction à la programmation en C”, tutorial class (38.5h), L1, Université Pierre et Marie Curie, France
- J. Lavauzelle, 2I011, “Méthodes numériques”, tutorial class (21h), L2, Université Pierre et Marie Curie, France
- J. Lavauzelle, 1I001, “Éléments de programmation”, tutorial class (38.5h), L1, Université Pierre et Marie Curie, France
- J. Lavauzelle, 2I003, “Initiation à l’algorithmique”, tutorial class (21.25h), L2, Université Pierre et Marie Curie, France
- A. Couvreur and E. Barelli, INF311, ”Introduction à l’informatique“, 26.7h(equiv TD), 1st year, Ecole Polytechnique, France.
- E. Barelli, INF411, "Les bases de la programmation et de l’algorithmique", 21.3h (equiv TD), 2nd year (L3), Ecole Polytechnique, France.
- B. Smith, INF442, "Traitement des données massives", 32h TD, 2nd year, École polytechnique
- A. Couvreur and B. Smith, INF411, "Les bases de la programmation et de l’algorithmique", 32h TD, 2nd year, École polytechnique

Master :

- D. Augot was mentoring François Bonnal, on a M1 research training projet, “bitcoin malleability”
- D. Augot was mentoring Édouard Dufour-Sans, on a M1 research training projet, “symmetric information theoretically secure private information retrieval schemes and applications”
- F. Levy-dit-Vehel, “Cours de Cryptographie”, 30h. (equiv TD), 3rd year (M1), ENSTA ParisTech, France.
- B. Smith, “Algorithmes arithmétiques pour la cryptologie”, 15h, MPRI (M2), Paris
- A. Couvreur, INF558a, “Introduction to cryptology”, 25h, Ecole Polytechnique (M1).
- A. Couvreur, “Introduction to coding theory and cryptology”, 10h, MPRI (M2), Paris.
- B. Smith supervised Nagarjun Chinthamani Dwarakanath for a 3A project and an M1 project on efficient curve-based cryptosystems at École polytechnique
- A. Couvreur supervised Evrim Petek’s M2 internship on the power decoding algorithm.
- A. Couvreur supervised Anas Aarab’s M1 TRE (*Travail de Recherche Encadré*) on the decoding of Reed Solomon codes.

Doctorat :

- Ben Smith made a lecture at the spring school on coding and cryptology at La Chapelle-Gauthier.

10.2.2. Supervision

- PhD in progress. J. Lavauzelle has began his Ph.D. on locally decodable codes and cryptogra[hic applications, on October 1st, 2015, under the supervision of D. Augot and F. Levy-dit-Vehel.
- PhD in progress. E. Barelli has begun his PhD on Algebraic-Geometry codes for code-based crypto on October 1st, 2015, under the supervision of D. Augot and A. Couvreur.
- PhD in progress. N. Duhamel has begun his PhD on genus 2 curves for cryptography, under the supervision of B. Smith and F. Morain.
- Completed PhD. P. Karpman, starting in 2013, defended in November 2016 his PhD on security of symmetric crytographic primitives.

10.2.3. Juries

- D. Augot was examiner in the jury of Fanny Jardel, who defended her thesis "Calcul et Stockage Distribués pour les Réseaux de Communication", January 11, Télécom-ParisTech
- D. Augot was examiner in the jury of Cécile Pierrot, who defended her thesis "Le logarithme discret dans les corps finis", November 25, Pierre and Marie Curie University.
- F. Morain was referee and examiner in the jury of Alexandre WALLET, who defended his thesis "Le problème de décomposition de points dans les variétés jacobiennes", December 14, Pierre and Marie Curie University.
- A. Couvreur is member of the jury of the agrégation de mathématiques and coordinator of option C ("algèbre et calcul formel).

10.3. Popularization

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

LFANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Selection

8.1.1.1. Member of the Conference Program Committees

A. Enge: 20th Workshop on Elliptic Curve Cryptography ECC 2016, İzmir

D. Robert was a member of the scientific committee for the Ecole Mathematique Africaine organised by Emmanuel Fouotsa at Bamenda.

F. Johansson organized the session: High-precision arithmetic, effective analysis and special functions. ICMS 2016, The 5th International Congress on Mathematical Software, ZIB Berlin.

8.1.2. Journal

8.1.2.1. Member of the Editorial Boards

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.

8.1.2.2. Reviewer - Reviewing Activities

F. Johansson reviewed for IEEE Transactions on Circuits and Systems I, IEEE Transactions on Computers, and ACM Transactions on Mathematical Software.

8.1.3. Invited Talks

- A. Enge: Mathematical Structures for Cryptography, Leiden: Short addition sequences for theta functions
- F. Johansson: talk at RAIM 2016, Banyuls-sur-mer on "Fast reversion of formal power series" and at FastRelax meeting, LAAS-CNRS, Toulouse on "Hypergeometric functions in Arb".

8.1.4. Scientific Expertise

J.-M. Couveignes is a member of the scientific council of the labex "Fondation Sciences Mathématiques de Paris", FSMP, Paris.

J.-M. Couveignes is a member of the 'conseil d'orientation' of the labex "Institut de Recherche en Mathématiques, Interactions et Applications", IRMIA, Strasbourg.

8.1.5. Research Administration

A. Enge: Head of COST-GTRI, responsible for the scientific evaluation of all international cooperations of Inria

Since January 2015, 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.

He is a member of the "Conseil National des Université" (25th section, pure mathematics).

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 2015, J.-M. Couveignes is the head of the Math Institute (IMB).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : G. Castagnos, *Cryptanalyse*, 60h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Cryptologie avancée*, 30h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

Master : D. Robert, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

8.2.2. Supervision

Pinar Kiliçer: The class number one problem for genus-2 curves, Universities of Bordeaux and Leiden, supervised by A. Enge, M. Streng and P. Stevenhagen.

Iuliana Ciocanea-Teodorescu, Algorithms for finite rings, Universities of Bordeaux and Leiden, supervised by K. Belabas and H. Lenstra.

PhD in progress: Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar, supervised by Djiby Sow, Abdoul Aziz Ciss and D. Robert.

PhD in progress: Emmanouil Tzortzakis *Algorithms for $\mathbb{Q}$-curves*, supervised by K. Belabas and P. Bruin

PhD in progress: Pavel Solomatin *Topics on L-functions*, supervised by B. de Smit and K. Belabas

Liu Zhengying: Height of class polynomials. Ecole Polytechnique third year internship, supervised by D. Robert.

8.2.3. Juries

- PhD report by A. Enge on Loubna Ghammam: Utilisation des couplages en cryptographie asymétrique pour la micro-électronique, University of Rennes
- PhD report and jury by D. Robert on Alina Dudeanu: Computational Aspects of Jacobians of Hyperelliptic Curves, EPFL.
- D. Robert is a member of the jury of Agregations de Mathematiques. He is also the codirector with Alain Couvreur of the option "calcul formel" of the Modelisation part of the oral examination.

8.3. Popularization

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

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

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

POLSYS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

Dongming Wang was involved in the organization of the following conferences

- Special Session on Software of Polynomial Systems at the 5th International Congress on Mathematical Software (ICMS 2016) (Berlin, Germany, July 11-14, 2016).

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

Emmanuel Prouff was member of the program committees of the following conferences

- Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016) (Santa Barbara, CA, USA, Aug. 17-19, 2016);
- Smart Card Research and Advanced Application Conference (CARDIS 2016) (Cannes, France, Nov. 7-9, 2016);
- International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2016) (Graz, Austria, Apr. 14-15);
- 23rd ACM Conference on Computer and Communications Security (ACM CCS 2016) (Vienna, Austria, Oct. 24-28).

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

- 11th International Workshop on Automated Deduction in Geometry (ADG 2016) (Strasbourg, France, June 27-29, 2016);
- 7th International Symposium on Symbolic Computation in Software Science (SCSS 2016) (Tokyo, Japan, March 28-31, 2016).

Elias Tsigaridas was member of the program committees of the following conferences

- Computer Algebra in Scientific Computing (CASC 2016), Sept 2016 Bucharest, Romania.

9.1.3. Journal

9.1.3.1. Member of the editorial boards

Ludovic Perret is Member of the Editorial Board of Designs, Codes and Cryptography.

Emmanuel Prouff is member of the editorial board of Journal of Cryptographic Engineering.

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

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),
- Member of the International Advisory Board for the Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).

9.1.4. Invited talks

Emmanuel Prouff was invited speaker at

- EUROCRYPT 2016 (invited tutorial), Vienna, Austria, on Securing Cryptography Implementations in Embedded Systems.
- SPACE 2016 (invited speaker), Hyderabad, India on Breaking Cryptographic Implementations Using Deep Learning Techniques.

Mohab Safey El Din was invited speaker at

- the SMAI-MODE session on semi-algebraic optimization, Toulouse, March 2016, France.
- the AIM Workshop on Algebraic Vision which was held at the American Institute of Mathematics, San Jose, May 2016, USA.
- the NCSU seminar on Symbolic Computation, Raleigh, May 2016, USA.
- the PGMO session on Semi-Definite Programming, Palaiseau, October 2016, France.

Ludovic Perret was invited speaker at 17th World Conference on Information Security Applications (WISA 2016, August, Korea).

Elias Tsigaridas was invited speaker at

- the Department Seminar Series, of the Computer Science Department of the University of Liverpool, Apr 2016, UK.
- the Seminar of RICAM, University of Linz, Austria (Dec. 2016)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Modeling and problems numerical and symbolic solving through MAPLE and MATLAB software, 34 hours, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Basics of Algebraic Algorithms, 70 hours, M1, Université Pierre-et-Marie-Curie, France

Master : Introduction to Security, 20 hours, M1, Université Pierre-et-Marie-Curie, France

Master : Projects supervision, 8 hours, L2, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Algorithmics, 49 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : Representations and Numerical Methods, 41 hours, L2, Université Pierre-et-Marie-Curie, France

Licence : Projects supervision, 10 hours, L2, Université Pierre-et-Marie-Curie, France

Jean-Charles Faugère had the following teaching activities:

Master: Fundamental Algorithms in Real Algebraic Geometry, 13,5 hours, M2, ENS de Lyon, France

Master : Polynomial Systems solving, 12 hours, M2, MPRI

Ludovic Perret had the following teaching activities amounting to around 220 hours:

Master : Polynomial Systems solving, M2, MPRI

Master : In charge of Introduction to Security, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Complexity, M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Algorithmic, L2, Université Pierre-et-Marie-Curie, France

Licence : In charge of the Computer Science – Applied Mathematics Program (PIMA) in Licence, L2, Université Pierre-et-Marie-Curie, France

Licence : Project supervision, L2, Université Pierre-et-Marie-Curie, France

Guénaël Renault had the following teaching activities:

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 45 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Advanced and Applied Cryptology, 70 hours, M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Security and Side-channels, 10 hours, M2, Université Pierre-et-Marie-Curie, France

Master : In charge of Threats and Attacks Modeling, 40 hours, M1, Université Pierre-et-Marie-Curie, France

Master : Pro/Research internships supervision, 40 hours, M2, Université Pierre-et-Marie-Curie, France

Master : Projects supervision, 20 hours, M1, Université Pierre-et-Marie-Curie, France

Licence : In charge of Introduction to Cryptology, 30 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : Project supervision, 10 hours, L2, Université Pierre-et-Marie-Curie, France

Mohab Safey El Din had the following teaching activities:

Master : In charge of Modeling and problems numerical and symbolic solving through MAPLE and MATLAB software, 36 hours, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Introduction to polynomial system solving, 48 hours, M2, Université Pierre-et-Marie-Curie, France

Master: In charge of Fundamental Algorithms in Real Algebraic Geometry, 22,5 hours, M2, ENS de Lyon, France

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 12 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

Master : Introduction to Security, 10 hours, M1, Université Pierre-et-Marie-Curie, France

Licence : Introduction to Cryptology, 20 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : In charge of the Computer Science – Applied Mathematics Program (PIMA) in Licence, L2 and L3, Université Pierre-et-Marie-Curie, France

9.2.2. Supervision

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

PhD in progress : Matías Bender, Algorithms for Sparse Gröbner basis and applications, started in Dec. 2015, Jean-Charles Faugère and Elias Tsigaridas

PhD in progress : Eleonora Cagli, Analysis and interest points research in the attacks by observation context, Emmanuel Prouff and Cécile Dumas

PhD in progress : Clayton Eduardo Lente da Silva, Planar discontinuous dynamical system, Universidade Estadual Paulista (São José do Rio Preto), started in Sep. 2013, Paulo Ricardo da Silva and Alain Jacquemard

HdR : Ludovic Perret, Université Pierre-et-Marie-Curie, defended in Dec. 2016

HdR : Guénaël Renault, Université Pierre-et-Marie-Curie, defended in Dec. 2016

PhD : Thársis Souza Silva, Relay Systems, Universidade Federal de Goiás, Goiânia, defended in May 2016, Ronaldo Alves Garcia and Alain Jacquemard

PhD : Adrian Thillard, Countermeasures to Side-Channel Attacks and Secure- Multi-Party Computation, ENS Paris, defended in Dec. 2016 Damien Vergnaud and Emmanuel Prouff

PhD : Thibaut Verron, Gröbner bases and structured polynomial systems, Université Pierre-et-Marie-Curie, defended in Sept. 2016, Jean-Charles Faugère and Mohab Safey El Din

PhD : Alexandre Wallet, The point decomposition problem in Jacobian varieties, Université Pierre-et-Marie-Curie, defended in Dec. 2016, Jean-Charles Faugère

9.2.3. Juries

Jean-Charles Faugère was examiner in the PhD committees of C. Chenavier, V. Neiger, T. Verron and A. Wallet and in the HDR committees of L. Perret and G. Renault.

Alain Jacquemard was examiner in the PhD committee of T.S. Silva.

Emmanuel Prouff was reviewer of the PhD theses of A. Battistello and D. Martin. He was examiner in the PhD committee of A. Battistello, D. Martin and A. Thillard and in the HDR committees of G. Renault.

Mohab Safey El Din was examiner in the PhD committees of T. Verron and A. Wallet and in the HDR committees of L. Perret and G. Renault.

9.3. Popularization

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

SECRET Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- DISC 2016, Workshop for early-career symmetric cryptographers funded by the COST Action IC1306, Bochum, Germany, March 23-24 2016. https://disc2016.compute.dtu.dk/, co-organizer: A. Canteaut.
- Research retreat (H2020 PQCRYPTO), September 21-22, 2016, Inria de Paris, organizer: N. Sendrier

10.1.1.2. Member of the Organizing Committees

- EuroS&P 2017: April 26-28, 2015, Paris (France): G. Leurent (poster chair)

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- FSE 2017: March 5-8, 2017, Tokyo, Japan: M. Naya-Plasencia (co-chair).

10.1.2.2. Member of the Conference Program Committees

- PQCrypto 2016: February 24-26, 2016, Fukuoka, Japan (N. Sendrier, J.P. Tillich)
- CT-RSA 2016: Feb. 29- March 4, 2016, San Francisco, USA (M. Naya Plasencia)
- FSE 2016: March 20-23, 2016, Bochum, Germany (A. Canteaut, G. Leurent)
- Eurocrypt 2016: May 8-12, 2016, Vienna, Austria (M. Naya Plasencia)
- Crypto 2016: August 14-18, 2016, Santa Barbara, USA (A. Canteaut)
- ACISP 2016: July 4-6, 2016, Melbourne, Australia (G. Leurent)
- Waifi 2016: July 13-15, 2016, Ghent, Belgium (A. Canteaut)
- YACC 2016: June 6-10, 2016, Porquerolles Island (A. Canteaut)
- SAC 2016: August 10-12, 2016, St. John's, NL, Canada (G. Leurent, M. Naya-Plasencia)
- Lightsec 2016: September 21-22, 2016, Cappadocia, Turkey (M. Naya-Plasencia)
- Redundancy 2016: September 26-29, 2016, St. Petersburg, Russia (P. Charpin)
- TQC 2016: September 27-29, 2016, Berlin, Germany (A. Chailloux);
- SETA 2016 (International Conference on SequEnces and Their Applications): October 9-14, 2016, Chengdu, China (P. Charpin).
- Asiacrypt 2016: December 4-8, 2016, Hanoi, Vietnam (A. Canteaut)
- Indocrypt 2016: December 11-14, 2016, Kolkata, India (G. Leurent)
- QIP 2017: January 16-20, 2017, Seattle, USA (A. Chailloux, A. Leverrier)
- Financial Crypto 2017: April 3-7, 2017, Sliema, Malta (G. Leurent)
- Fq13: June 4-9, 2017, Geata, Italy (A. Canteaut)
- Crypto 2017: August 20-24, 2017, Santa Barbara, CA, USA (G. Leurent)

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- *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.
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut.
- *IACR Transactions on Symmetric Cryptology*, associate editors: A. Canteaut and G. Leurent, co-editor-in-chief: M. Naya-Plasencia.

P. Charpin serves as a reviewer for *Mathematical Reviews*.

10.1.3.2. Editor for books or special issues

- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, to appear, editors: P. Charpin, N. Sendrier and J-P. Tillich.
- *Contemporary Developments in Finite Fields and Applications*, 2016, World Scientific Publishing [62], co-editor: A. Canteaut.

10.1.4. Invited Talks

- G. Leurent *Breaking Symmetric Cryptosystems Using Quantum Period Finding*, TCCM-CACR 2016, Yinchuan, China, August 2016
- A. Leverrier, *Quantum Expander Codes*, Beyond i.i.d. in Information Theory, Barcelone, Spain, 18-22 June 2016

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

- A. Canteaut, *Another view of the division property* Dagstuhl seminar on symmetric cryptology, Dagstuhl, Germany, Jan. 10-14, 2016.
- A. Canteaut, *Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression*, CryptoAction Symposium 2016, Budapest, Hungary, April 6-8, 2016.
- A. Canteaut, *Algebraic Distinguishers against Symmetric Primitives*, Paris Crypto Day, France, June 30, 2016.
- A. Canteaut, *Comment concevoir un algorithme de chiffrement sûr et efficace : l'héritage de Shannon*, Shannon 100, workshop organized at the occasion of Shannon's 100th birthday, Institut Henri Poincaré, Paris October 26, 2016. The talk is available online at https://www.youtube.com/watch?v=BYlOO4MkVgU.
- A. Chailloux, *Cryptographie relativiste*, Coding, Cryptography and Algorithms (CCA), Paris, July 1, 2016.
- A. Chailloux, *Quantum Information Processing*, Journées Scientifiques Inria 2016, Rennes, France, June 2016.
- V. Lallemand, *Cryptanalysis of the FLIP Family of Stream Ciphers*, Paris Crypto Day, Sept. 6, 2016.
- G. Leurent, *Transcript Collision Attacks*, Dagstuhl seminar on symmetric cryptology, Dagstuhl, Germany, Jan. 10-14, 2016.
- A. Leverrier, *Distributing Secret Keys with Quantum Continuous Variables*, Recent Advances in Continuous-variable Quantum Information Theory, Barcelone, Spain, 16-8 April 2016
- M. Naya-Plasencia: *Pourquoi essaie-t-on de casser les fonctions cryptographiques ?*. Colloquium organised by the pre-GDR Sécurité Informatique: Colloque Sécurité informatique CNRS http://colloque-cybersecu.cnrs.fr/. Paris, France, Dec. 9, 2016.
- J.P. Tillich, *Attaining the capacity with Reed-Solomon codes through the* $(U|U+V)$ *construction and Koetter-Vardy soft decoding*, Journée Claude Shannon, Paris, July 1, 2016.

10.1.5. Leadership within the Scientific Community

- 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;
- N. Sendrier is a member of the "Comité de pilotage" of the ANR (défi 9);
- Since 2014, JP. Tillich organizes a working group on code-based cryptography which meets on a monthly/bimonthly basis. It gathers people from the project-team, from the GRACE project-team (Inria Saclay), from the University of Limoges, from the University of Rennes and from the University of Rouen who all work on this topic.

10.1.6. Research Administration

- N. Sendrier has been a vice-chair of the "Commission d'Evaluation" at Inria until October 2016;
- A. Canteaut is a member of the "Comité de pilotage" of the Fondation Sciences Mathématiques de Paris;
- M. Naya-Plasencia is a member of *Inria Paris CES Committee* (Comité de suivi doctoral).
- M. Naya-Plasencia is a member of *Inria Paris Scientific Hiring Committee* (Assignement of PhD, post-doctoral and delegation Inria fundings).
- N. Sendrier served on the jury of PEDR CNRS INSII 2016.
- J.-P. Tillich is in charge of "Formation par la recherche" for the Paris Inria center;
- **Committees for the selection of professors, assistant professors and researchers**: Inria Paris Chargés de recherche (A. Canteaut), University Paris 8 assistant professor (A. Canteaut, M. Naya-Plasencia, JP Tillich), Inria Directeurs de recherche (N. Sendrier)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

Master: A. Canteaut, *Error-correcting codes and applications to cryptology*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Chailloux, *Quantum computing*, 6 hours, M2, University Paris-Diderot (MPRI), France;

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

Master: N. Sendrier, Information theory, 32 hours, M1, University of Versailles-St Quentin (MINT), 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 summer schools for PhD students:

- *UbiCrypt Spring School on Symmetric Cryptography*, Bochum, Germany, March 2016: A. Canteaut (9 hours). Some of the lectures are available online.

E-learning

Mooc: I. Marquez-Corbella and N. Sendrier, *Code-based cryptography*, 5 weeks, FUN, Inria, undergraduate and Master's degree students in mathematics or computer science.

Pedagogical resources: https://www.fun-mooc.fr/courses/inria/41006S02/session02/about

10.2.2. Supervision

PhD: Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, University Pierre-et-Marie Curie, October 5, 2016, supervisors: M. Naya-Plasencia and A. Canteaut

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

PhD in progress: Rodolfo Canto Torres, *Analysis of generic decoding algorithms for the Hamming metric and study of cryptosystems based on the rank metric*, since September 2015, supervisor: N. Sendrier

PhD in progress: Sébastien Duval, *Constructions for lightweight cryptography*, since October 2015, supervisor: A. Canteaut and G. Leurent

PhD in progress: Yann Rotella, *Finite fields and symmetric cryptography*, since October 2015, supervisor: A. Canteaut

PhD in progress: Xavier Bonnetain, *Cryptanalysis of symmetric primitives in the post-quantum world*, since September 2016, supervisor: M. Naya Plasencia and A. Canteaut

PhD in progress: Thomas Debris, *Quantum algorithms for decoding linear codes*, since September 2016, supervisor: J.-P. Tillich

PhD in progress: Antoine Grospellier, *LDPC codes: constructions and decoding*, since October 2016, supervisor: J.-P. Tillich

PhD in progress: Vivien Londe, *Study of quantum LDPC codes*, since September 2016, supervisors: G. Zémor and A. Leverrier

PhD in progress: Kevin Carrier, *Reconstruction of error-correcting codes*, since October 2016, supervisor: N. Sendrier

10.2.3. Juries

- Mohamed Nidhal Mejri, *Securing Vehicular Networks against Denial of Service attacks*, University Paris 13, May 19, 2016, committee: A. Canteaut;
- Tung Chou *Accelerating Pre- and Post-quantum Cryptography*, TU Eindhoven, The Netherlands, June 26, 2016, committee: N. Sendrier;
- Jean-Marie Le Bars, *Some studies about randomness in Computer Science*, HdR, University of Caen, June 29, 2016, committee: J.P. Tillich (reviewer);
- Tom Douce, *Realistic quantum information processing: from devices to computational models*, Université Paris Diderot, September 9, 2016, committee: A. Leverrier;
- Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, University Pierre-et-Marie Curie, October 5, 2016, committee: M. Naya-Plasencia and A. Canteaut (supervisors)
- Brice Minaud, *Analysis of recent cryptographic primitives*,University of Rennes 1, October 7, 2016, committee: A. Canteaut;
- Pierre Karpmann, *Analysis of symmetric primitives*, University Paris-Saclay, October 18, 2016, committee: A. Canteaut (reviewer);
- Jean-Christophe De Neuville, *Contributions to post-quantum cryptography*, University of Limoges, December 1, 2016, committee: J.P. Tillich (reviewer).
- Zoé Amblard , *Quantum cryptography and applications to spatial communications*, University of Limoges, December 5, 2016, committee: J.P. Tillich (reviewer).
- Qian Guo, *Using coding techniques for attacking post-quantum cryptographic assumptions and systems*, Lund University, Sweden, December 13, 2016, committee: J.P. Tillich.

10.3. Popularization

- Nicolas Sendrier and Jean-Pierre Tillich, *Code-Based Cryptography: New Security Solutions Against a Quantum Adversary*, ERCIM News [67].
- Anne Canteaut gave a talk at the *dotSecurity 2016* conference for developers, at Théâtre des Variétés, Paris, April 2016 http://www.thedotpost.com/2016/05/anne-canteaut-the-struggle-for-secure-cryptography.
- Anne Canteaut gave a talk at *Séminaire général du département d'informatique de l'ENS* for Master students in computer science at ENS Paris, April 13, 2016 http://savoirs.ens.fr/expose.php?id=2516.
- André Chailloux gave a talk entitled *L'ordinateur quantique*, at Journées Art, Cerveau, Futur; Mouans-Sartoux, France, September 2016;

- Anne Canteaut gave a talk on cryptography at lycée Rodin, Paris, February 2, 2016.
- Sébastien Duval gave a talk on cryptography at lycée des 7 Mares, Maurepas, December 2, 2016
- Anne Canteaut has been involved in the AlKindi competition, which is a national competition on cryptanalysis for students in “Seconde” http://www.concours-alkindi.fr/.

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

SPECFUN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Frédéric Chyzak is member of the steering committee of the *Journées Nationales de Calcul Formel* (JNCF), the annual meeting of the French computer algebra community.
- Frédéric Chyzak has been elected member of the steering committee of the *International Symposium on Symbolic and Algebraic Computation* (ISSAC, 3-year term).
- Alin Bostan is part of the Scientific advisory board of the conference series *Effective Methods in Algebraic Geometry* (MEGA).
- Assia Mahboubi serves in the scientific advisory board of the Mathematics, Algorithms and Proofs community (MAP).
- Assia Mahboubi has served in the scientific advisory board of the École du GDR Informatique – Mathématiques 2016.
- Georges Gonthier is a member of the steering committee of the *Certified Programs and Proofs* conference (CPP).

9.1.1.2. Member of the Organizing Committees

- Assia Mahboubi has co-organized the *MAP'16 conference* at CIRM (Marseille), with B. Spitters (Aarhus University, Denmark) and P. Schuster (University of Verona, Italy): http://scientific-events.weebly.com/1508.html.
- Assia Mahboubi has co-organized, with E. Tassi (Marelle), the workshop *Mathematical Components: an introduction*, satellite of the conference ITP 2016: https://itp2016.inria.fr/workshops/#mc.
- Assia Mahboubi has co-organized, with K. Nakata (FireEye, Germany), the workshop *TTT*, satellite of the POPL'17 conference: http://popl17.sigplan.org/track/TTT-2017.
- Suzy Maddah has co-organized the gathering *Functional Equations in Limoges (FELIM 2016)*: https://indico.math.cnrs.fr/event/919/.
- Suzy Maddah has co-organized a session on software for the symbolic study of functional equations at the *International Congress on Mathematical Software (ICMS 2016)*: http://icms2016.zib.de/.
- Alin Bostan has co-organized, together with Bruno Salvy (Inria and ENS Lyon) and Conrado Martinez (UPC BarcelonaTech), the conference *ALEA 2016* at CIRM (Marseille): http://scientific-events.weebly.com/1406.html.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Alin Bostan has served as Symbolic Computation track chair for the international conference SYNASC 2016.

9.1.2.2. Member of the Conference Program Committees

- Assia Mahboubi has served as a member of the program committee for the international conferences with proceedings CPP 2017, ITP 2016, CSL 2016, CICM 2016 and SCSS 2016. She has also served as member of the program committee for the MAP 2016 conference and for the HaTT workshop.
- Alin Bostan has served as a member of the program committee of the ISSAC 2016 and of the SYNASC 2016 international conferences.

9.1.2.3. Reviewer

- Assia Mahboubi has served as reviewer for the proceedings of the international conferences CPP 2017, ITP 2016, CSL 2016, CICM 2016 and SCSS.
- Alin Bostan has served as reviewer for the proceedings of the international conferences FPSAC 2016, ISSAC 2016, AofA 2016 and SYNASC 2016.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Georges Gonthier is a member of the editorial board of the *Journal of Formalized Reasoning*.

9.1.3.2. Reviewer - Reviewing Activities

- Assia Mahboubi has served as a reviewer for the *Journal of Automated Reasoning*.
- Frédéric Chyzak has served as a reviewer for the journals: *Applicable Algebra in Engineering, Communication and Computing*; *Journal of Symbolic Computation*; *Journal of Algebra*; and *Electronic Journal of Combinatorics*.
- Alin Bostan has served as a reviewer for the journals: *Journal of Complexity*; *Mathematics of Computation*; *Linear Algebra and its Applications*; *Journal of Physics A: Mathematical and Theoretical*; *Journal of Algebra and its Applications*; *Journal of Symbolic Computation*; *Advances in Applied Mathematics*.

9.1.4. Invited Talks

- Assia Mahboubi has given an invited talk at the special trimester Mathematics – Computer Science – Philosophy CIPPMI in Toulouse in March 2016.
- Assia Mahboubi has given an invited lecture for the students of École Normale Supérieure Paris-Saclay in September 2016.
- Alin Bostan has been invited to give a series of five lectures at the summer school *Algorithmic and Enumerative Combinatorics* (RISC, Hagenberg, Austria), August 1–5, 2016.
- Philippe Dumas has given an invited lecture about divide-and-conquer recurrences at the *Journées Aléa* (CIRM, Marseille, France), March 7–11, 2016 [18].

9.1.5. Leadership within the Scientific Community

- Assia Mahboubi is leading the working group *Type theory based tools* inside the EUTYPES COST project. She is also M.C. for France for this project and a member of its core managment group.

9.1.6. Research Administration

- Assia Mahboubi is member of the *Commission Scientifique* of Inria Saclay — Île-de-France.
- Georges Gonthier is a member of the board of the *École doctorale de mathématiques Hadamard (EDMH)*.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

License:

Louis Dumont, two L1 maths courses, 64h, Université Paris-Sud, France.

Master:

Assia Mahboubi, *Proof Assistants*, 18h, M2, Denis Diderot University (Paris), France.

Frédéric Chyzak, *Algorithmes efficaces en calcul formel*, 18h, M2, MPRI, France.

Alin Bostan, *Algorithmes efficaces en calcul formel*, 40.5h, M2, MPRI, France.

Pierre Lairez, *Algorithmique avancée*, 18h, M1, École polytechnique, France.

9.2.2. Supervision

PhD in progress: Thomas Sibut-Pinote, "Calcul numérique et démonstrations mathématiques: de la rigueur à la preuve formelle", September 2014, Assia Mahboubi

PhD in progress: Louis Dumont, "Algorithmes rapides pour le calcul symbolique de certaines intégrales de contour à paramètre", started in September 2013, supervised by Alin Bostan and B. Salvy.

Master intership (M1): G. Boisseau and Th. Huffschmitt, *Combination of decision procedures in presence of meta-variables*, École Polytechnique, supervised by Assia Mahboubi (jointly with S. Graham-Lengrand from LIX).

9.2.3. Juries

- Alin Bostan has served as a jury member of the French *Agrégation de Mathématiques – épreuve de modélisation, option C*.
- Alin Bostan has served as an examiner in the PhD jury of Aladin Virmaux, *Théorie des représentations combinatoires de tours de monoïdes, Application à la catégorification et aux fonctions de parking*, Université Paris-Saclay, June 13, 2016.

9.3. Popularization

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

VEGAS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of Organizing Committees

Sylvain Lazard organized with S. Whitesides (Victoria University) the 15th Workshop on Computational Geometry at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

Monique Teillaud co-organized the workshop *20 years of CGAL*, with Efi Fogel, Michael Hoffmann, and Emo Welzl, Zurich, Switzerland, September 10-11, and she gave a talk.

9.1.2. Scientific Events Selection

9.1.2.1. Member of Conference Program Committees

Monique Teillaud was a member of the program committee of EuroCG, *European Workshop on Computational Geometry*.

9.1.2.2. Reviewer

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.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Monique Teillaud is a managing editor of JoCG, *Journal of Computational Geometry*. She is also a member of the Editorial Board of IJCGA, *International Journal of Computational Geometry and Applications*. She resigned from the Editorial Board of CGTA, *Computational Geometry: Theory and Applications*, after unsuccessfully trying to convince the Editorial Board to leave Elsevier and move to a free (libre and gratis) open-access model.

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

Olivier Devillers resigned from the Editorial Board of Graphical Models (Elsevier) after discussion to move to a free open-access model.

9.1.3.2. Reviewer - 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.

9.1.4. Invited Talks

Olivier Devillers was invited to give a talk at the geometry week organized by GipsaLab in Grenoble.

Guillaume Moroz was invited to give talks at the LIGM seminar in Marne-la-Vallée university, at the SpecFun team seminary in Inria Saclay and at the MSDOS workshop in CIRM.

Monique Teillaud was invited to give a talk talk at the seminar *Computer Science meets Mathematics* of the University of Luxembourg, February 8: "CGAL, geometry made practical". She was invited to give a talk at the *Mittagsseminar* of Institute of Theoretical Computer Science of ETH Zürich on September 8: "Delaunay triangulations on orientable surfaces of low genus".

9.1.5. Seminar Organization

We invited:

Kacper Pluta (LIGM - Laboratoire d'Informatique Gaspard-Monge),

Mickaël Buchet (Tohoku University).

Andrew Yarmola (University of Luxembourg).

9.1.6. Leadership within the Scientific Community

9.1.6.1. Steering Committees

M. Teillaud has been elected Chair of the Steering Committee of the Symposium on Computational Geometry (SoCG). She is a member of the Steering Committee of the European Symposium on Algorithms (ESA).

9.1.7. Research Administration

9.1.7.1. Hiring committees

Sylvain Lazard was president of the hiring committee for a Professor position (UL/École des Mines/LORIA).

Monique Teillaud was the representative of LORIA in the hiring committee for an Associate Professor (MCF) position (École des Mines/LORIA) and composed the committee with the president. She was also a member of the Inria CR2 Nancy - Grand Est interview committee and of the hiring committee for a Professor position (FST/LORIA).

9.1.7.2. National committees

L. Dupont is a member of "Commission Pédagogique Nationale" (CPN) Information-Communication / Métiers du Multimédia et de l'Internet.

M. Teillaud is a member of the Scientific Board of the *Société Informatique de France* (SIF).

M. Teillaud is a member of the working group for the BIL, *Base d'Information des Logiciels* of Inria.

9.1.7.3. Local Committees and Responsabilities

S. Lazard: Head of the PhD and Post-doc hiring committee for Inria Nancy-Grand Est (since 2009). Member of the *Bureau de la mention informatique* of the *École Doctorale IAE+M* (since 2009). Head of the *Mission Jeunes Chercheurs* for Inria Nancy-Grand Est (since 2011). Head of the Department Algo at LORIA (since 2014). Member of the *Conseil Scientifique* of LORIA (since 2014).

G. Moroz is member of the Mathematics Olympiades committee of the Nancy-Metz academy. G. Moroz is member of the *Comité des utilisateurs des moyens informatiques*

M. Pouget is elected at the *Comité de centre*, and member of the board of the Charles Hermite federation of labs. M. Pouget is secretary of the board of *AGOS-Nancy*.

M. Teillaud is a member of the BCP, *Bureau du Comité des Projets* and of the CDT, *Commission de développement technologique* of Inria Nancy - Grand Est.

9.1.7.4. Websites

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/international Symposium on Computational Geometry.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : O. Devillers, *Synthèse, image et géométrie* , 12h (academic year 2015-16) and 12h (academic year 2016-2017), IPAC-R, Université de Lorraine. https://members.loria.fr/ODevillers/master/

Master: Marc Pouget, *Introduction to computational geometry*, 10.5h, M2, École Nationale Supérieure de Géologie, France.

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

Licence: Laurent Dupont, *Algorithmique*, 78h, L1, Université de Lorraine, France.

Licence: Laurent Dupont, *Web development*, 75h, L2, Université de Lorraine, France.

Licence: Laurent Dupont, *Traitement Numérique du Signal*, 10h, L2, Université de Lorraine, France.

Licence: Laurent Dupont, *Data structures*, 40h, L1, Université de Lorraine, France.

9.2.2. Supervision

PhD : Ranjan Jha, Étude de l'espace de travail des mécanismes à boucles fermées, defended in Jul. 2016, 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 in progress : Charles Duménil, Probabilistic analysis of geometric structures, started in Oct. 2016, supervised by Olivier Devillers.

PhD in progress : Iordan Iordanov, Triangulations of Hyperbolic Manifolds, started in Jan. 2016, supervised by Monique Teillaud.

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

9.2.3. Juries

O. Devillers was president of the PhD defense committee of Vincent Despré (Univ. Grenoble-Alpes).

G. Moroz was in the PhD defense committee of Ranjan Jha (IRCCyN).

9.2.4. Teaching Responsabilities

Licence: Laurent Dupont, creation and opening of L3 (Licence Professionnelle) « Animation des Communautés et Réseaux Socionumériques », Université de Lorraine, France.

CAIRN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. General Chair, Scientific Chair

E. Casseau was General Co-Chair of DASIP, Conference on Design and Architectures for Signal and Image Processing, October 12-14, 2016.

S. Derrien was Co-Chair of WRC, 10th HiPEAC Workshop on Reconfigurable Computing, January 18-20, 2016 (co-located with HiPEAC 2016).

T. Yuki was Co-Chair of IMPACT, 6th International Workshop on Polyhedral Compilation Techniques, January 18-20, 2016 (co-located with HiPEAC 2016).

9.1.1.2. Chair of Conference Program Committees

O. Sentieys was Track Chair at IEEE NEWCAS.

9.1.1.3. Member of the Conference Program Committees

D. Chillet was member of the technical program committee of HiPEAC RAPIDO, HiPEAC WRC, MCSoC, DCIS, ComPAS, DASIP, LP-EMS, ARC.

S. Derrien was a member of technical program committee of IEEE FPL and ARC conferences and of WRC and Impact workshops.

O. Sentieys was a member of technical program committee of IEEE/ACM DATE, IEEE FPL, ACM ENSSys, ACM SBCCI, IEEE ReConFig, CROWNCOM, FSP, FPGA4GPC.

T. Yuki was a member of technical program committee of SC'16, The International Conference for High Performance Computing, Networking, Storage and Analysis.

9.1.2. Journal

9.1.2.1. Member of the Editorial Boards

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 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, Inderscience.

9.1.3. Invited Talks

O. Sentieys gave an invited talk at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Villard-de-Lans, France, in January 2016 on "Approximate Computing and Flexible Circuits for the IoT".

T. Yuki gave a half-day lecture at EJCP 2016, École Jeunes Chercheurs en Programmation, Lille.

T. Yuki gave an invited talk at University of Arizona in June 2016 on "Optimizing Compilers in High-Level Synthesis".

9.1.4. Leadership within the Scientific Community

D. Chillet is member of the Board of Directors of Gretsi 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).

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

O. Sentieys is a member of the steering committee of the GDR SOC-SIP.

9.1.5. Scientific Expertise

O. Sentieys served as a jury member in the EDAA Outstanding Dissertations Award (ODA).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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)

E. Casseau: advanced processor architectures, 25h, Univ. of Science and Tech. of Hanoi (M2)

S. Derrien: component and system synthesis, 20h, Master by Research (MRI ISTIC) (M2)

S. Derrien: computer architecture, 12h, ENS Rennes (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 Univ. of Science and Tech. of Hanoi (M1)

D. Chillet: embedded processor architecture, 20h, ENSSAT (M1)

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

D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne (M2)

C. Killian: digital electronics, 62h, IUT Lannion (L1)

C. Killian: signal processing, 36h, IUT Lannion (L2)

C. Killian: automated measurements, 56h, IUT Lannion (L2)

C. Killian: measurement chain, 35h, IUT Lannion (L2)

C. Killian: embedded systems programming, 12h, IUT Lannion (L2)

C. Killian: automatic control, 9h, IUT Lannion (L2)

A. Kritikakou: computer architecture 1, 50h, ISTIC, Univ. Rennes 1 (L3)

A. Kritikakou: computer architecture 2, 50h, ISTIC, Univ. Rennes 1 (L3)

A. Kritikakou: operating systems 1, 24h, ISTIC, Univ. Rennes 1 (L3)

A. Kritikakou: operating systems 2, 64h, ISTIC, Univ. Rennes 1 (L3)

A. Kritikakou: multitasking operating systems, 45h, ISTIC, Univ. Rennes 1 (M1)

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

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

O. Sentieys: high level synthesis, 16h, Master by Research (SISEA) and ENSSAT (M2)

A. Tisserand: multiprocessor architectures, 20h, ENSSAT and Master by Research (SISEA) (M2)

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)

9.2.2. Teaching Responsibilities

C. Wolinski is the Director of ESIR.
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" major of the SISEA Master by Research.
D. Chillet is the responsible of the ICT Master of University of Science and Technology of Hanoi.
C. Killian is the responsible of the second year of the Physical Measurement DUT at IUT of Lannion.

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.

9.2.3. Supervision

PhD: Florent Berthier, Study and Design of an Ultra Low Power Asynchronous Core for Sensor Networks, Dec. 2016, O. Sentieys, E. Beigne.

PhD: Ali Hassan El-Moussawi, Performance/Accuracy Trade-Off in Automatic Parallelization for Embedded Many-Core Platforms, Dec. 2016, S. Derrien.

PhD: Jérémie Métairie, Reconfigurable Arithmetic Units for Secure Cryptoprocessors, May 2016, A. Tisserand, E. Casseau.

PhD in progress: Benjamin Barrois, Approximate Computing: a New Paradigm for Energy-Efficient Computing Architectures, Oct. 2014, O. Sentieys.

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: Gabriel Gallin, Hardware Arithmetic Units and Crypto-Processor for Hyperelliptic Curves Cryptography, Oct. 2014, A. Tisserand.

PhD in progress: Aymen Gammoudi, New Visual Adaptive Real-Time OS for Embedded Multi-Core Architecture, Oct. 2015, D. Chillet, M.Khalgui.

PhD in progress: Mael Gueguen, Improving the performance and energy efficiency of complex heterogeneous manycore architectures with on-chip data mining, Nov. 2016, O. Sentieys, A. Termier.

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: Audrey Lucas, Software support resistant to passive and active attacks for asymmetric cryptography on (very) small computation cores, Jan. 2016, A. Tisserand.

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: Genevieve Ndour, Approximate Computing with High Energy Efficiency for Internet of Things Applications, Apr. 2016, A. Tisserand, A. Molnos (CEA LETI).

PhD in progress: Joel Ortiz Sosa, Study and design of a digital baseband transceiver for wireless network-on-chip architectures, Nov. 2016, O. Sentieys, C. Roland (Lab-STICC).

PhD in progress: Kleanthis Papachatzopoulos, Predictable and fault-tolerant multicore architecture, Oct. 2016, A. Kritikakou, O. Sentieys.

PhD in progress: Tara Petric, Approximate@runtime: Playing with accuracy at run-time for low-power flexible circuits in IoT nodes, Nov. 2016, T. Yuki, O. Sentieys.

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: Rafail Psiakis, A Self-Healing Reconfigurable Accelerator Structure for Fault-Tolerant Multi-Cores, Oct. 2015, A. Kritikakou, O. Sentieys.

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

PhD in progress: Simon Rokicki, Hybrid Hardware/Software Dynamic Compilation for Adaptive Embedded Systems, Oct. 2015, S. Derrien.

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: Nicolas Roux, Sensor-aided Non-Intrusive Appliance Load Monitoring: Detecting Activity of Devices through Low-Cost Wireless Sensors, Oct. 2016, O. Sentieys, B. Vrigneau.

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.

CAMUS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Selection

10.1.1.1. Member of the Conference Program Committees

Cédric Bastoul has been part of the program committee of IMPACT 2016 (International Workshop on Polyhedral Compilation Techniques), held in conjunction with the international conference HiPEAC 2016.

Philippe Clauss and Cédric Bastoul have been part of the program committee of IMPACT 2017 (International Workshop on Polyhedral Compilation Techniques), held in conjunction with the international conference HiPEAC 2017.

Alain Ketterlin has been part of the program committee of CGO 2016 (International Symposium on Code Generation and Optimization, http://cgo.org/cgo2016).

Cédric Bastoul and Vincent Loechner have been part of the program committee of both HIP3ES 2016 and HIP3ES 2017 (International Workshop on High Performance Energy Efficient Embedded Systems), held in conjunction with the international conference HiPEAC 2016 (resp. HiPEAC 2017).

Cédric Bastoul has been part of the program committee of PARMA+DITAM 2016 and PARMA+DITAM 2017 (Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures + Workshop on Design Tools and Architerctures for Multicore Embedded Computing Platforms), held in conjunction with HiPEAC 2016 (resp. HiPEAC 2017).

Cédric Bastoul has been part of the program committee of the international conference on Compiler Construction 2017 (CC'2017).

10.1.1.2. Reviewer

Philippe Clauss has been reviewer for the following conferences and workshops: IMPACT 2017 (International Workshop on Polyhedral Compilation Techniques), CC 2017 (International Conference on Compiler Construction).

Cédric Bastoul has been reviewer for the following international conferences and workshops: CC 2017 (International Conference on Compiler Construction), PARMA 2016 and 2017 (International Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures), IMPACT 2016 and 2017 (International Workshop on Polyhedral Compilation Techniques), HIP3ES 2016 and 2017 (International Workshop on High Performance Energy Efficient Embedded Systems).

Vincent Loechner has been reviewer for CC 2017 (International Conference on Compiler Construction), HIP3ES 2016 and 2017 (International Workshop on High Performance Energy Efficient Embedded Systems).

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

Since October 2001, J. Gustedt is Editor-in-Chief of the journal *Discrete Mathematics and Theoretical Computer Science* (DMTCS).

10.1.2.2. Reviewer - Reviewing Activities

Philippe Clauss has been reviewer for the following journals: ACM TACO (Transactions on Architecture and Code Optimization), Parallel Computing.

Cédric Bastoul has been reviewer for the *ACM Transactions on Parallel Computing International Journal* (TOPC).

Jens Gustedt has been reviewer for Theory of Computing Systems.

Vincent Loechner has been reviewer for *Computer Communications* (Elsevier).

10.1.3. Invited Talks

Philippe Clauss has been invited to present the framework Apollo at the Parallel Programming Laboratory of the University of Darmstadt, Germany, October the 28th.

Philippe Clauss has presented the framework Apollo at the COSI research group of the Colorado State University, Fort Collins, USA, July the 1st.

10.1.4. Scientific Expertise

Cédric Bastoul as been an expert for the French research ministry and the French finance ministry for the research tax credit programme.

Jens Gustedt served as expert for project evaluation for the Belgian FNRS, and as evaluator of the FEMTO-ST Lab, Besançon, for the French HCERES.

10.1.5. Standardization

Since Nov. 2014, Jens Gustedt is a member of the ISO working group SC22-WG14 for the standardization of the C programming language. He participates actively in the defect report processing, the planning of future versions of the standard, and publishes an ongoing document to track inconsistencies and improvements of the C threads interface.

This work on the C programming language also gave rise to the proposal of a language extension, Modular C. It has been used for the implementation of an efficient toolbox for *higher order automatic differenciation*, `arbogast`, see [18] and [19], which has been presented at the quadrennial conference of the domain, AD2016.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence : Philippe Clauss, Architecture des ordinateurs, 45h, Université de Strasbourg, France

Licence : Philippe Clauss, Systèmes d'exploitation, 40h, Université de Strasbourg, France

Master : Philippe Clauss, Compilation, 78h, Université de Strasbourg, France

Master : Philippe Clauss, Système et programmation temps-réel, 25h, Université de Strasbourg, France

Master : Philippe Clauss, Compilation avancée, 30h, Université de Strasbourg, France

Licence : Éric Violard, Programmation Fonctionnelle (licence informatique), 64h eq. TD, L2, Université de Strasbourg, France

Licence : Éric Violard, Architecture des Ordinateurs (licence informatique), 54h eq. TD, L2, Université de Strasbourg, France

Licence : Éric Violard, Logique et Programmation Logique (licence informatique), 34h eq. TD, L2, Université de Strasbourg, France

Licence : Éric Violard, Algorithmique et Structures de Données (licence mathématique), 39h eq. TD, L3, Université de Strasbourg, France

Licence : Éric Violard, Modèles de Calcul (licence informatique), 29h eq. TD, L1, Université de Strasbourg, France

Licence : Vincent Loechner, Systèmes d'exploitation, 51h, L2, Université de Strasbourg, France

Master : Vincent Loechner, parallélisme, 14h, M1, Université de Strasbourg, France

Master : Vincent Loechner, calcul parallèle, 32h, M1, Université de Strasbourg, France

Master : Vincent Loechner, langages interprétés, 37h, M1, Université de Strasbourg, France

Master : Vincent Loechner, OS embarqués, 31h, M2, Université de Strasbourg, France

Telecom Physique Strasbourg : Vincent Loechner, calcul parallèle, 20h, M2, Université de Strasbourg, France

Licence : Alain Ketterlin, Systèmes d'exploitation, 20h, Université de Strasbourg, France

Licence : Alain Ketterlin, Systèmes Concurrents, 24h, Université de Strasbourg, France

Licence : Alain Ketterlin, Réseaux et protocoles, 42h, Université de Strasbourg, France

Master : Alain Ketterlin, Compilation, 26h, Université de Strasbourg, France

Licence : Cédric Bastoul, Architecture, 68h, L1 (IUT), Université de Strasbourg, France

Licence : Cédric Bastoul, Operating Systems, 16h, L2, Université de Strasbourg, France

Licence : Cédric Bastoul, Concurrent Systems, 19h, L3, Université de Strasbourg, France

Master : Cédric Bastoul, Compiler Design, 48h, M1, Université de Strasbourg, France

Master : Cédric Bastoul, Parallelism, 16h, M1, Université de Strasbourg, France

Master : Cédric Bastoul, Introduction to Research, 7h, L3+M1, Université de Strasbourg, France

2nd year engineering school: Jens Gustedt, programmation avancée, 20h, ENSIIE Strasbourg, France

Licence : Jens Gustedt, systèmes concurrents, 20h, Université de Strasbourg, France

10.2.2. Supervision

PhD: Tomasz Buchert, Madynes team, *Orchestration of experiments on distributed systems*, since Oct 2011, defended on Jan 6 2016, Jens Gustedt & Lucas Nussbaum.

PhD: Juan Manuel Martinez Caamaño, *Fast and Flexible Compilation Techniques for Effective Speculative Polyhedral Parallelization*, September 29th 2016, Philippe Clauss and Philippe Helluy (IRMA lab., University of Strasbourg)

PhD: Michel Massaro, *Méthodes numériques pour les plasmas sur architectures multicœurs*, December 16th 2016, Philippe Helluy and Vincent Loechner

PhD: Lénaïc Bagnères, Adaptation automatique et semi-automatique des optimisations de programmes, September 30th, Christine Eisenbeis and Cédric Bastoul

PhD: Olexander Zinenko, Interactive Program Restructuring, November 25th 2016, Stéphane Huot and Cédric Bastoul

PhD in progress: Yann Barsamian, *Optimization and parallelization of particle and semi-Lagrangian methods for multi species plasma simulations*, since Oct 2014, Éric Violard

PhD in progress: Mariem Saied, *Ordered Read-Write Locks for Multicores and Accelerators*, since Nov 2013, Jens Gustedt & Gilles Muller.

PhD in progress: Daniel Salas, *Integration of the ORWL model into parallel applications for medical research*, since Mar 2015, Jens Gustedt & Isabelle Perseil.

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

PhD in progress: Harenome Ranaivoarivony-Razanajato, *Hierarchical Optimization and Parallelization*, September 2016, Vincent Loechner and Philippe Clauss

PhD in progress: Maxime Schmitt, *Automatic Generation of Adaptive Codes*, September 2016, Cédric Bastoul and Philippe Helluy

PhD in progress: Paul Godard, *Parallelization and Scalability of an Image Processing Pipeline for Professional Printing*, September 2016, Vincent Loechner and Cédric Bastoul

10.2.3. Juries

Philippe Clauss participated to the following PhD committees in 2016:

Date	Candidate	Place	Role
Jun. 30	Guillaume Iooss	Colorado State Univ., USA	Reviewer
Oct. 28	Zhen Li	Univ. Darmstadt, Germany	Reviewer
Sept. 29	Juan Manuel Martinez Caamaño	Univ. Strasbourg	Advisor
Dec. 14	Julien Pagès	Univ. Montpellier	Reviewer

Cédric Bastoul participated to the following PhD committees in 2016:

Date	Candidate	Place	Role
June 22	Abdul Memon	Paris-Saclay University	Reviewer
September 30	Lénaïc Bagnères	Paris-Saclay University	Advisor
November 18	Albert Saa	Universitat Autònoma de Barcelona	Reviewer
November 25	Oleksandr Zinenko	Paris-Saclay University	Advisor
November 30	Pierre Guillou	Paris Sciences et Lettres Research University	Reviewer

Vincent Loechner participated to the following PhD committees in 2016:

Date	Candidate	Place	Role
May 10	Arjun Suresh	Univ. Rennes 1	Examiner
December 16	Michel Massaro	Univ. Strasbourg	Co-advisor

Vincent Loechner was the president of the recruiting jury (*comité de sélection*) for an assistant professor position at the Department of Mathematics and Computer Science of the University of Strasbourg, during Spring 2016.

10.3. Popularization

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

COMPSYS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Alain Darte is general chair of the steering committee of CPC (International Workshop on Compilers for Parallel Computing), which regroups in Europe, every 18 months, a large community of researchers interested in compilers for HPC. He participated to CPC'16 in Valladolid in July 2016.

10.1.1.2. Member of the Organizing Committees

Tomofumi Yuki was co-organizer of IMPACT'16 (International Workshop on Polyhedral Compilation Techniques, http://impact.gforge.inria.fr/impact2016/) with Michelle Strout (University of Arizona).

10.1.1.3. Spring School on Numerical Simulation and Polyhedral Compilation

Alain Darte (with the help of Tomofumi Yuki for the program) co-organized with Violaine Louvet (Institute Camille Jordan in Lyon, now lead of UMS Gricad in Grenoble) a second polyhedral spring school, May 9-13 2016, targeting both the polyhedral community and HPC users from numerical analysis. This spring school has been labelled (and funded) as a CNRS interdisciplinary spring school (https://mathsinfohpc.sciencesconf.org/), with a total budget of roughly 39 Keuros, including funding from Labex MILYON, CNRS, GDR Calcul, ENS, LIP, and registrations fees, which were kept low to keep the spirit of the first spring school on polyhedral code analysis and optimizations.

This second spring school was motivated by the need for a more global approach for HPC applications, that combines the design of numerical methods with extensive hardware considerations, in interaction with languages and compilers, so as to take into account both the complexity of architectures and the needs of their non-expert users. Research communities in computer science (architecture, compilation) and applied mathematcs (numerical simulation) are not always aware of this need; at least their work do not always spread enough across the other discipline to lead to mutual influence. Automatic code optimizations and tools also require a better evaluation of their applicability. The goal of this research school – or meeting place of two communities – was to make the link between some of the most recent advances on automatic program optimizations (in particular polyhedral techniques and tools) and applied mathematics (schemes for numerical simulation), in relation with application needs. This school was therefore interdisciplinary, with a strong will to bring communities together on the common theme of supercomputing.

We finally opted for a single track instead of parallel sessions, which helped federate the two communities. The school included courses on architectures (M. Haefele, Maison de la simulation), on numerical schemes in connection with stencils (T. Dumont, ICJ), on simulation methods (discontinuous Galerkin) in particular for GPU (P. Helluy, Strasbourg), on polyhedral techniques and tiling (A. Darte, Compsys), on some polyhedral compilers such as Pluto (U. Bondhugula, Bangalore) and PPCG (S. Verdoolaege, ENS), on the roofline model for performance analysis (M. Püschel, ETH Zürich), on stencils and tensors optimizations (Ramanujam, Baton Rouge), on numerical precision (C. Rubio-Gonzalez, UC Davis), plus some additional talks on reproducibility, applications, the ECM model, etc. The school was a success, with 71 participants, roughly half from each community, with 29 coming from abroad (Italy, Algeria, USA, India, Canada, Germany, Croatia, Switzerland, Austria, Belgium), and a majority (37) being PhD students.

The future will tell if our objectives have been reached, i.e., if the two communities will interact more on the long term and rethink their work with an interdisciplinary look, to invent new computing schemes and compilers more suitable for the constraints of today's architectures, in particular their memory hierarchy and locality needs. In Compsys at least, one can already see some moves in this direction, with the interdisciplinary internship of Julien Versaci co-advised by Tomofumi Yuki, the participation of Alain Darte as a referee to the PhD jury of T. Gasc (CEA, Maison de la Simulation, ENS Cachan), a planned seminar by Alain Darte at Maison de la Simulation in early 2017, starting exchanges with the LMGC lab (Montpellier) on their applications, and a planned mini-symposium, following the line of this spring school, at SMAI 2017.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

In addition to the organization, Tomofumi Yuki was program co-chair of IMPACT'16, with Michelle Strout (University of Arizona).

10.1.2.2. Member of the Conference Program Committees

Alain Darte was a member of the program committee of HPCS'16 (International Conference on High Performance Computing & Simulation) and will be member of the program committee of PACT'17 (International Conference on Parallel Architectures and Compilation Techniques).

Paul Feautrier was a member of the program committees of IMPACT'16 and IMPACT'17.

Tomofumi Yuki was a member of the program committees of SC'16, X10 Workshop'16, IMPACT'16, and IMPACT'17.

10.1.2.3. Reviewer

Alain Darte, Paul Feautrier, and Tomofumi Yuki were reviewers for the different program committees to which they participated.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

No participation to journal editorial boards in 2016.

10.1.3.2. Reviewer - Reviewing Activities

Alain Darte was a reviewer for the "Software, Practice, and Experience" journal.

Paul Feautrier was a reviewer for the "International Journal of Parallel Programming".

Tomofumi Yuki was a reviewer for the TACO, TOPLAS, JPDC, and TPDS journals.

10.1.4. Invited Talks

Alain Darte was invited to give a talk on "Liveness Analysis in Explicitly-Parallel Programs" at ScalPerf'16 in Bertinoro (Italy), Sep. 2016.

Paul Feautrier was invited to give a talk (in two parts) "Toward A Polynomial Model with Application to the OpenStream Language" at the second and third LCS (Language, Compilation, Semantics) LIP seminars, in June and November 2016.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master:

- Paul Feautrier was invited to give a talk on "New Architectures, New Compilations Problems", at the student seminar for the IMAG M2 course, Grenoble, December 5, 2016.

Spring/Summer Schools:

- Alain Darte, as part of the spring school on numerical simulation and polyhedral compilation, gave a half-day course on "Introduction to Automated Polyhedral Code Optimizations and Tiling", see https://mathsinfohpc.sciencesconf.org.
- Tomofumi Yuki, a part of the École Jeunes Chercheurs en Programmation 2016, gave a half-day course on "Research in Compilers and Introduction to Loop Transformations", see http://ejcp2016.univ-lille1.fr/.

10.2.2. Supervision

PhD: Guillaume Iooss, "Detection of linear algebra operations in polyhedral programs" [16], joint PhD ENS-Lyon/Colorado State University, started Sep. 2011, defended July 1st, 2016, advisors: Christophe Alias and Alain Darte (ENS-Lyon) / Sanjay Rajopadhye (Colorado State University).

PhD: Alexandre Isoard, "Extending Polyhedral Techniques towards Parallel Specifications and Approximations" [17], ENS-Lyon, started in Sep. 2012, defended July 5th, 2016, advisor: Alain Darte.

Guillaume Iooss is now post-doc in the Parkas team, while Alexandre Isoard is R&D engineer at Xilinx (Dublin, Ireland, then San Jose, Ca).

10.2.3. Juries

Alain Darte was one of the two reviewers of the PhD of Thibault Gasc (CEA DAM DIF, Maison de la Simulation, November 2016), entitled "Modèles de performance pour l'adaptation des méthodes numériques aux architectures multi-cœurs vectorielles. Application aux schémas Lagrange-Projection en hydrodynamique compressible". He was also member of the juries of the PhD of Alexandre Isoard, as adviser, and of Guillaume Iooss as administrative co-adviser.

10.3. Popularization

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

CORSE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Ylies Falcone: 1st international summer school on Runtime Verification; 3rd international Competition on Runtime Verification
- Frédéric Desprez: EuroPAR 2016 (co-chair and workshop chair)

9.1.1.2. Member of the Organizing Committees

- Fabrice Rastello: Program Committee ACM/IEEE CGO 2015; Steering Committee Journées française de la compilation; Steering Committee ACM/IEEE CGO

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Fabrice Rastello: Program Chair ACM/IEEE CGO 2016; Program Chair "Journées française de la compilation", Aussois, 2016
- Ylies Falcone: Program Chair RV 2016

9.1.2.2. Member of the Conference Program Committees

- Fabrice Rastello: ACM CC 2016, ACM SRC SC 2016, ACM/IEEE SRC SC 2016
- Alain Ketterlin: ACM/IEEE CGO 2016
- Ylies Falcone: CARI 2016, SSS 2016, RV 2016, Pre-Post'16, SAC-SVT'16
- Frédéric Desprez: Closer 2016, CCGrid 2016, HPC 2016, EuroPAR 2016, CloudCom 2016

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

- Fabrice Rastello: ACM TACO
- Ylies Falcone: Formal Aspects of Computing, ACM Transactions on Automatic and Control, Acta Informatica, Formal Methods in System Design, International Journal of Information and Computer Security, Science of Computer Programming, Software Tools for Technology Transfer, Journal of Systems and Software, NFM 2016

9.1.4. Invited talks

- Fabrice Rastello: UCDenver: "Toward Automatic Characterisation of the Data Access Complexity of Programs"
- Ylies Falcone: American University of Beirut: "On the Runtime Enforcement of Timed Properties"
- Ylies Falcone: LAAS Toulouse: "On the Runtime Enforcement of Timed Properties"
- Frédéric Desprez: Inria Alumni: "Internet des objets, Où sont les ruptures? Activités à l'Inria"
- Frédéric Desprez: SUCCES Workshop: "CIMENT, GRICAD, Grid'5000: La synergie grenobloise"
- Frédéric Desprez: CCDSC Workshop: "BOAST: Performance Portability Using Meta-Programming and Auto-Tuning"
- Frédéric Desprez: Eurecom Seminar 2016: "Challenges and Issues of Next Cloud Computing Platforms"

- Frédéric Desprez: European Commission, Brussels: "Research Issues for Future Cloud Infrastructures"
- Frédéric Desprez: CIRM, CEMRACS 2016 summer school: "OpenCL Introduction"
- François Broquedis: CIRM, CEMRACS 2016 summer school: "A Gentle Introduction to OpenMP Programming"
- Jean-François Méhaut: CEMRACS 2016 summer school: "Overview of architectures and programming language for parallel computing"

9.1.5. Scientific expertise

- Frédéric Desprez: European project in the FP7 framework
- Frédéric Desprez: Comité d'orientation stratégique de CIRRUS (COMUE Paris)
- Frédéric Desprez: Groupe Technique GENCI
- Frédéric Desprez: Conseil Scientifique GIS France Grille
- Frédéric Desprez: GENCI, expert for grants of computing resources (CT6)
- Ylies Falcone: Representative of France in the COST Action ARVI
- Ylies Falcone: COST Action ARVI, co-leader of Working Group on Core Runtime Verification
- Jean-François Mehaut: Eurolab-4-HPC, expert for cross site mobility research grants
- Jean-François Mehaut: GENCI, expert for grants of computing resources (CT6)

9.1.6. Research administration

- Frédéric Desprez: Deputy Scientific Director at Inria
- Frédéric Desprez: Director of the GIS GRID5000
- Frédéric Desprez: Conseil Scientifique ESIEE Paris

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master II: Fabrice Rastello, Advanced Compilers, 12 hours, ENS Lyon

Master I: Jean-François Méhaut, Operating System Design, 50 hours, Polytech Grenoble

L3: Jean-François Méhaut, Numerical Methods, 50 hours, Polytech Grenoble,

L3: Jean-François Méhaut, Advanced Algorithms, 50 hours, Polytech Grenoble

L3: François Broquedis, Imperative programming using python, 40 hours, Grenoble Institute of Technology (Ensimag)

L3: François Broquedis, C programming, 80 hours, Grenoble Institute of Technology (Ensimag)

M1: François Broquedis, Operating systems and concurrent programming, 40 hours, Grenoble Institute of Technology (Ensimag)

M1: François Broquedis, Operating Systems Development Project - Fundamentals, 20 hours, Grenoble Institute of Technology (Ensimag)

M1: François Broquedis, Operating Systems Project, 20 hours, Grenoble Institute of Technology (Ensimag)

Master: Florent Bouchez Tichadou, Compilation project, 15 hours, M1 Info & M1 MoSig

Licence: Florent Bouchez Tichadou, C programming, 24 hours, L3, Grenoble Institute of Technology (Ensimag)

Master: Florent Bouchez Tichadou, Algorithmic Problem Solving, 41 hours, M1 MoSIG

Licence: Florent Bouchez Tichadou, Algorithms languages and programming, 121 hours, L2 UGA

Licence: Florent Bouchez Tichadou is responsible of the second year of INF (informatique) and MIN (mathématiques et informatique) students at UGA

Master I: Ylies Falcone Proof Techniques and Logic Reminders, MoSIG, 3 hours

Master I: Ylies Falcone Recaps on Object-Oriented Programming, MoSIG, 3 hours

Master II: Ylies Falcone Introduction to Runtime Verification, MoSIG HECS, 8 hours.

Master I: Ylies Falcone Programming Language Semantics and Compiler Design, MoSIG, 66 hours

License: Ylies Falcone Languages and Automata, UJF, 105 hours

Master: Ylies Falcone is co-responsible of the first year of the International Master of Computer Science (Univ. Grenoble Alpes and INP ENSIMAG)

9.2.2. Supervision

9.2.2.1. Fabrice Rastello

PhD defended [3]: Duco van Amstel, Scheduling and optimization for memory locality of dataflow programs on many-core processors, advised by Fabrice Rastello and Benoit Dupont-de-Dinechin

PhD defended [1]: Diogo Sampaio, Profiling Guided Hybrid Compilation, October 8 2013, advised by Fabrice Rastello

PhD defended: Venmugil Elango, Dynamic Analysis for Characterization of Data Locality Potential, advised by Fabrice Rastello and P. Sadayappan.

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: Fabian Grüber, Interactive & iterative performance debugging, September 2016, advised by Fabrice Rastello and Ylies Falcone.

PhD in progress: Philippe Virouleau, *Improving the performance of task-based runtime systems on large scale NUMA machines*, co-advised by Thierry Gautier (Inria/AVALON), Fabrice Rastello, François Broquedis

9.2.2.2. Jean-François Méhaut

PhD defended (April 2016): Oleg Iegorov, advised by Alexandre Termier (Dream/Irisa), Vincent Leroy (SLIDE/LIG) and Jean-François Méhaut

PhD defended (October 2016): Nassim Halli, CIFRE with Asselta, advised by Henri-Pierre Charles (CEA/DRT List), Jean-François Méhaut

PhD defended [36]: Naweiluo Zhou, advised by Eric Rutten (Inria, CtrlA), Gwenael Delaval (UGA, CtrlA), Jean-François Méhaut

PhD in progress: Thomas Messi Nguelé, advised by Maurice Tchuenté (Yaoundé I, LIRIMA) and Jean-François Méhaut

PhD in progress: Thomas Goncalves, advised by Marc Perache (CEA/DAM), Frédéric Desprez, Jean-François Méhaut

PhD in progress: Luis Felipe Milani, advised by Lucas Schnoor (UFRGS), François Broquedis and Jean-François Méhaut

PhD in progress: Vanessa Vargas, advised by Raoul Velazco (CNRS, TIMA) and Jean-François Méhaut

PhD in progress: Raphaël Jakse, Monitoring and Debugging Component-Based Systems, advised by Jean-François Mehaut and Ylies Falcone.

9.2.2.3. Frédéric Desprez

PhD defended (October 2016): Jonathan Pastor, advised by Frédéric Desprez, Adrien Lèbre (EMN Nantes, Ascola team)

PhD in progress: Pedro Silva, advised by Frédéric Desprez, C. Perez (Inria, Avalon team)

PhD in progress: Georgios Christodoulis, advised by Frederic Desprez, Olivier Muller (TIMA/SLS) and François Broquedis

PhD in progress: Thomas Goncalves, advised by Marc Perache (CEA/DAM), Frédéric Desprez, Jean-François Méhaut

PhD in progress: Ye Xia, advised by Thierry Coupaye (Orange), Frédéric Desprez, Xavier Etchevers (Orange)

9.2.2.4. François Broquedis

PhD in progress: Georgios Christodoulis, *Adaptation of a heterogeneous runtime system to efficiently exploit FPGA* advised by Frederic Desprez, Olivier Muller (TIMA/SLS) and François Broquedis

PhD in progress: Philippe Virouleau, *Improving the performance of task-based runtime systems on large scale NUMA machines*, co-advised by Thierry Gautier (Inria/AVALON), Fabrice Rastello, François Broquedis

9.2.2.5. Ylies Falcone

PhD in progress: Hosein Nazarpour, Monitoring Multithreaded and Distributed Component-based Systems, advised by Saddek Bensalem (Vérimag) and Ylies Falcone.

PhD in progress: Antoine El-Hokayem, Decentralised and Distributed Monitoring of Cyber-Physical Systems, advised by Ylies Falcone.

PhD in progress: Fabian Grüber, Interactive & iterative performance debugging, September 2016, advised by Fabrice Rastello and Ylies Falcone.

PhD in progress: Raphaël Jakse, Monitoring and Debugging Component-Based Systems, advised by Jean-François Mehaut and Ylies Falcone.

9.2.3. Juries

9.2.3.1. Fabrice Rastello

Venmugil Elango, Advisor, *Dynamic Analysis for Characterization of Data Locality Potential*, PhD of OSU, 06/01/2016

Arjun Suresh, Reviewer, *Intercepting Functions for Memoization*, PhD of Université de Rennes, 10/04/2016

Duco Van-Amstel, Advisor, *Scheduling and optimization for memory locality of dataflow programs on many-core processors*, Université Grenoble Alpes, 11/07/2016.

Juan Manuel Martinez Caamano, Reviewer, *Fast and Flexible Compilation Techniques for Effective Speculative Polyhedral Parallelization*, Université de Strasrbourg, 29/09/2016

Pierre Guillou, Reviewer, *Compilation efficace d'applications de traitement d'images pour processeurs manycore*, Université de recherche PAris Sciences et Lettres, 30/11/2016

9.2.3.2. Jean-François Méhaut

Oleg Iegorov, Advisor,*Data Mining Approach to Temporal Debugging of Embedded Streaming Applications*, PhD of Université Grenoble Alpes, April 2016

Nassim Halli, Advisor, *Code Optimizations of High Performance Java Applications*, PhD of Université Grenoble Alpes, October 2016

Naweiluo Zhou, Advisor, *Autonomic Thread Parallelism and Mapping Control for Software Transactional Memory System*, PhD of Université Grenoble Alpes, October 2016

Marc Sergent, Reviewer, *Passage à l'échelle d'un support d'exécution à base de tâches pour l'algèbre linéaire creuse*, PhD of Université de Bordeaux, October 2016

Jean-Charles Papin, Reviewer, *A Scheduling and Partitioning Model for Stencil-based Applications on ManyCore Devices*, PhD of Ecole Normale Supérieure de Cachan, July 2016

9.2.3.3. Frédéric Desprez

Jean-Marie Couteyen, Reviewer, *Parallélisation et passage à l'échelle du code FLUSEPA*, PhD of Université de Bordeaux, September 2016

Jonathan Pastor, Advisor, *Contributions à la mise en place d'une infrastructure de Cloud Computing à large échelle* , Ecole des Mines de Nantes, October 2016

DREAMPAL Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Selection

8.1.1.1. Member of the Conference Program Committees

V.Rusu was a member in the PC of the 2016 edition of the Int. Workshop on Rewriting Logic and Applications, and will be the organizer of the next edition of the event. He was was also PC member of Approches Formelles pour la Validation Logicielle (AFADL'2016).

8.1.2. Research Administration

Vlad Rusu is elected member at Inria's Evaluation Committee. As such he has been involved in several activities regarding promotions of researchers, team creations, and team evaluations.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : V.Rusu, Logic, 30hrs, L3, Univ. Lille, France.

Doctorat : V. Rusu, External adviser for PhD students, Univ. Iasi, Romania.

PACAP Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

A. Seznec is member of the ACM/IEEE PACT conference steering committee.

A. Seznec is member of the ACM/IEEE ISCA symposium steering committee.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Isabelle Puaut is Program Chair of the 2017 IEEE Real-Time Systems Symposium (RTSS).

A. Seznec was PC chair of the 2016 ACM/IEEE ISCA symposium.

10.1.2.2. Member of the Conference Program Committees

Isabelle Puaut is member of the program committees of the Euromicro Conference on Real Time Systems (ECRTS) 2016 and 2017, the IEEE Real-Time Systems Symposium (RTSS) 2016, the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2017 and the WCET workshop 2016.

A. Seznec is a member of IEEE Micro 2017 Top Picks selection committee.

A. Seznec was a member of the SAMOS 2016 conference program committee.

Damien Hardy was a member of RTNS 2016 and WCET 2016 program committees.

Pierre Michaud was a member of the program committees of the HPCA 2017 conference and of the 5th JILP Workshop on Computer Architecture Competitions (JWAC-5).

Sylvain Collange was PC member of ISCA 2016 and of Compas'2016.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Isabelle Puaut is Associate Editor for IEEE Transactions on Computers (IEEE TC).

A. Seznec is a member of the editorial boards of IEEE Micro and ACM Transactions on Architecture and Compiler Optimization.

10.1.4. Invited Talks

Damien Hardy was invited to give a tutorial on Heptane at Tutor16 (1st Tutorial on Tools for Real-Time Systems) in conjunction with the Cyber-Physical Systems week 2016.

Damien Hardy was invited from August 31st to September 2nd at the Barcelona Supercomputing Center group. He presented an invited talk.

A. Seznec presented invited talks at Intel Bangalore (compressed caches, branch prediction, value prediction) in Sept. 2016.

A . Seznec presented the PACAP work on compressed caches at the ARM research summit in Sept. 2016.

A. Seznec presented the PACAP work on compressed caches and register equality prediction at the Intel low latency ISRA workshop in Dec. 2016.

10.1.5. Scientific Expertise

Erven Rohou was an expert for the ANR review process.

10.1.6. Research Administration

Isabelle Puaut is responsible of Short Term Scientific Missions (STSM) withing the European COST action Tacle (Timing Analysis at Code LEvel) (http://www.tacle.eu).

Isabelle Puaut is member of the steering committee of RTNS (Real-Time Networks and Systems).

Isabelle Puaut is member of the steering committee of the Worst Case Execution Time (WCET) workshop, held in conjunction with the Euromicro Conference on Real Time Systems (ECRTS).

Isabelle Puaut is member of the scientific council of University of Rennes 1.

Isabelle Puaut is member of the administration council of the computer science and electrical engineering department of University of Rennes 1.

A. Seznec is an elected member of the Administration Council of Inria.

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).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Isabelle Puaut, Operating systems, 1st year of master, total of 110 hours

Master: Isabelle Puaut, Damien Hardy, Real-time systems, 1st year of master, total of 58 hours

Master: Isabelle Puaut, Erven Rohou, Writing of scientific publications, 2nd year of master and PhD students, total of 24 hours

Licence: Damien Hardy, Real-time systems, L3 Université de Rennes I, total of 60 hours

Master: Damien Hardy, Operating systems, M2 Université de Rennes I, total of 60 hours

Master: Damien Hardy, Operating systems, M1 Université de Rennes I, total of 60 hours

Master: S. Collange, Programmation parallèle, 22 hours, M1, Université de Rennes I, France

10.2.2. Supervision

PhD: Sajith Kalathingal, "Transforming TLP into DLP with the Dynamic Inter-Thread Vectorization Architecture", Université Rennes 1, Dec 2016, co-advisors S. Collange and A. Seznec

PhD: Aswinkumar Sridharan, "Adaptive and Intelligent Memory Systems", Université Rennes 1, Dec. 2016, advisor A. Seznec

PhD: Arjun Suresh, "Intercepting Functions for Memoization", Université Rennes 1, May 2016, co-advisors E. Rohou and A. Seznec

PhD in progress, Viet Anh Nguyen, Worst-Case Execution Time (WCET) Estimation for Many-core Architectures, started in january 2015. Supervised by Isabelle Puaut and Damien Hardy.

PhD in progress, Benjamin Rouxel, Code optimizations for WCET calculation on many-core platforms, started in october 2015. Supervised by Isabelle Puaut and Steven Derrien from the CAIRN group.

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

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

PhD in progress: Rabab Bouziane, Université Rennes 1, Nov 2015, advisor E. Rohou and Abdoulaye Gamatié (LIRMM, Montpellier)

PhD in progress: Arif Ali Ana-Pparakkal, Université Rennes 1, Feb 2015, advisor E. Rohou

PhD in progress: Simon Rokicki, Université Rennes 1, Sep 2015, co-advisors E. Rohou and Steven Derrien (CAIRN)

PhD in progress: Kleovoulos, Kalitzidis, "Ultrawide Issue Superscalar Processors", Université Rennes 1, Dec. 2016, advisor A. Seznec

10.2.3. Juries

Isabelle Puaut was a member of the following committees:

- PhD: Pierre Wilke, Formally Verified Compilation of Low-Level C code, Université de Rennes 1, Nov 2016
- PhD: Guillaume Phavorin, Hard Real-Time Scheduling subjected to Cache-Related Preemption Delays, Université de Poitiers, Sep 2016 (rapporteur)
- PhD: Vincent Mussot, Automates d'annotation de flot pour l'expression et l'intégration de propriétés dans l'analyse de WCET, Université Paul Sabatier, Toulouse, Dec 2016 (rapporteur)
- HDR: Mathieu Jan, Contributions au paradigme par cadencement temporel (TT) et à l'embarquabilité des systèmes temps réel, Université Paris Sud, Dec 2016 (rapporteur)

Erven Rohou was a member of the following committees:

- PhD: Juan Manuel Martinez Caamano, Strasbourg
- PhD: Lénaïc Bagnères, Orsay
- PhD: Michele Scandale, Politecnico di Milano, Milan, Italy
- PhD: Amir Ashouri, Politecnico di Milano, Milan, Italy
- PhD: Sébastien Martinez, Télécom Bretagne, Brest
- PhD: Reem ElKhouly, Egypt-Japan University of Science and Technology, Alexandrie, Egypt

10.2.3.1. Assistant professor hiring committees

Isabelle Puaut: University of Toulouse (computer architecture and real-time systems)

Isabelle Puaut: University of Chalmers, Sweden (real-time systems)

10.2.3.2. Professor hiring committee:

Isabelle Puaut: UBO (Université de Bretagne Occidentale) - real-time systems

10.3. Popularization

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

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

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

TASC Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Leadership within the Scientific Community

Charlotte Truchet was elected in the ACP committee.

10.1.2. Research Administration

Preparation by the whole team of the two evaluations that respectively toke place in January 2016 (hceres evaluation) and in March 2016 (inria evaluation).

10.2. Teaching - Supervision - Juries

10.2.1. Supervision

PhD: Ignacio Salas Donoso, Packing curved objects with interval methods, Started in May 2013, PhD defense April 5 2016 with committee Luc Jaulin, Gilles Trombettoni, François Fages, see PhD thesis, Gilles Chabert and Nicolas Beldiceanu.

PhD in progress : Gilles Madi Wamba, Mixing constraint programming and behavioural models to manage energy consumption in data centre, October 2014, Nicolas Beldiceanu and Didier Lime.

PhD in progress : Alejandro Reyes Amaro, Toward autonomous parallel algorithms for constraint-based problems, October 2014, Eric Monfroy and Florian Richoux.

PhD in progress : Anicet Bart, Solving mixed constraints, application to the management of mobile sensors, October 2014, Eric Monfroy and Charlotte Truchet.

PhD in progress : Ekaterina Arafailova, Functional constraints, September 2015, Nicolas Beldiceanu and Rémi Douence.

PhD in progress : Nicolas Galvez, Hybrid Algorithms for Search Based Software Engineering, December 2014, Eric Monfroy with Frédéric Saubion from Angers University and C. Castro from UTFSM Valparaiso, Chili.

10.3. Popularization

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

AOSTE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Eric Madelaine is General Chair of the 11th International Symposium on Theoretical Aspects of Software Engineering (TASE'17), and Steering Committee Chair of the International Symposium on Formal Aspects of Components Systems (FACS 2017)
Liliana Cucu-Grosjen and Rob Davis are Steering Committee members of 3 conferences (RTSS, RTAS and RTNS) and 2 workshops (RTSOPS and WMC)
Julien Deantoni was chair of the 4th GEMOC workshop, held in conjunction with the 19th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Robert de Simone will be PC Chair for the forthcoming EMSoft 2017 conference edition.
Frédéric Mallet will be PC Chair for the forthcoming TASE 2017 conference edition.

9.1.2.2. Member of the Conference Program Committees

Robert de Simone: EmSoft 2016, FDL 2016.
Dumitru Potop-Butucaru: RTNS 2016, ACSD 2016
Yves Sorel: DASIP 2016, EMSOFT 2016
Julien Deantoni: MODELS 2016, CAL 2016, GEMOC 2016, EXE 2016 DSD 2016, MOMO 2016.
Liliana Cucu-Grosjean: RTAS2016, SIES 2016, RTNS2016
Fredéric Mallet: DATE 2016, DSD 2016, ERTS 2016, ICTERI 2016.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Yves Sorel: DASIP 2016, EMSOFT 2016

9.1.4. Invited Talks

Robert de Simone was invited Keynote Speaker at the international conference MeMoCode 2016 in Kanpur (India)

9.1.5. Leadership within the Scientific Community

Eric Madelaine and Frédéric Mallet are Council Members of the International Joint Laboratory of Trustworthy Software, Ministery of Education, China.

9.1.6. Scientific Expertise

Yves Sorel: Steering Committees of System Design and Development Tools Group of Systematic Paris-Region Cluster, and of Technologies and Tools Program of SystemX Institute for Technological Research (IRT)

9.1.7. Research Administration

Robert de Simone is Scientific Correspondant for the Inria/Safran collaboration programme, and (starting 2017) Deputy Director of the EDSTIC Doctoral School of Université Côte d'Azur.
Liliana Cucu-Grosjean is elected member of Inria Evaluation Commission.

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 Internationbal, UNS.

Master: Robert de Simone, Functional and Temporal Correctness, 36h, M1 Internationbal, UNS.

Master: Yves Sorel, Optimization of distributed real-time embedded systems, 36H, M2, University of Paris Sud

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

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, Finite State Machines, 24h, M1,Polytech'Nice, France.

Master : Julien Deantoni, Internship Management, 20h, M2, Polytech'Nice, France.

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, Conception Orientée Objet, 45h, L3, UNS.

Licence: Frédéric Mallet, Programmation Orientée Objet, 45h, L3, UNS.

Master: Frédéric Mallet, Programmation Avancée et Design Patterns, 45h, M1, UNS.

Master: Frédéric Mallet, Vérification temporelle et fonctionnelle, 24h, M1, UNS.

Master: Frédéric Mallet, Model-Driven Engineering, 24h, M1, UNS.

Master: Liliana Cucu, Distributed Databases and Statistics in Computer Science, 64h, U. Dunarea de Jos, Romania (Invited Professor)

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

9.2.2. Supervision

PhD: Matias Vara-Larsen, *Toward a formal and hierarchical timed model for concurrent heterogeneous model*, UNS, defended April 2016, 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, defended May 2016, supervised by Robert de Simone.

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: Yuanrui Zhang, ECNU-SEI/China, started Sep 2015, co-supervised by Frederic Mallet (joint supervision with Pr. Chen Yixiang(ECNU).

PhD in prgress: Hui (Vincent) Zhao, UNS, started February 2016, supervised by Frédéric Mallet, co-supervised by Ludovic Apvrille (Telecom ParisTech)

PhD in progress: Dongdong An, ECNU-SEI/China, started November 2016, co-supervised by R. de Simone, supervised by Jing Liu (ECNU).

PhD in progress: Cristian Maxim, *End to end constraints using probabilistic approaches*, UPMC, started on March 2014, supervised by Liliana Cucu

PhD in progress: Walid Talaboulma, *Probabilistic timing analysis in presence of dependences*, UPMC, started on November 2015, co-supervised by Liliana Cucu and Adriana Gogonel

PhD in progress: Salah Edinne Saidi, *Distributed real-time scheduling for the co-simulation of several control models*, University of UMPC-Paris-Sorbonne, started December 2014, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel.

PhD in progress: Keryan Didier, *Formal certification of real-time implementations*, Université Pierre et Marie Curie/EDITE, started November 2015, supervised by Dumitru Potop Butucaru.

PhD: Oleksandra Kulankhina, *A framework for rigorous development of distributed components: formalisation and tools*, UNS, defended October 2016, supervised by Eric Madelaine, co-supervised by Ludovic Henrio (UMR CNRS/UNS I3S).

PhD in progress: Salah Edinne Saidi, *Distributed real-time scheduling for the co-simulation of several control models*, University of UMPC-Paris-Sorbonne, started December 2014, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel.

PhD in progress: Keryan Didier, *Formal certification of real-time implementations*, Université Pierre et Marie Curie/EDITE, started November 2015, supervised by Dumitru Potop Butucaru.

PhD: Oleksandra Kulankhina, *A framework for rigorous development of distributed components: formalisation and tools*, UNS, defended October 2016, supervised by Eric Madelaine, co-supervised by Ludovic Henrio (UMR CNRS/UNS I3S).

PhD: Vincent Kherbache, *Ordonnancement des migrations à chaud de machines virtuelles*, UNS, defended December 2016, supervised by Eric Madelaine, co-supervised by Fabien Hermenier (UMR CNRS/UNS I3S).

9.2.3. Juries

Robert de Simone: reviewer for the HDR of Xavier Thirioux (ENSIIEHT, Sept. 2016)

Dumitru Potop Butucaru: PhD reviewer for Pierre Guillou - Ecole des Mines de Paris. Nov. 2016

Julien Deantoni: PhD reviewer for Florent Latombe (ENSIIEHT)

Liliana Cucu-Grosjean: PhD reviewer for Guillaume Phavorin (ENSMA Poitiers, September 2016)

Liliana Cucu-Grosjean: PhD jury member for Abhilash Thekkilakattil (University of Ma¨lardalen, May 2016)

9.3. Popularization

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

CONVECS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

- H. Garavel is a member of the model board [0] of MCC (*Model Checking Contest*). In 2016, he helped preparing new models (especially those in the NUPN format) and verified, using the CÆSAR.BDD tool of CADP, the forms describing all benchmark models submitted by the contest participants; this revealed a number of inconsistencies. The mission and activities of the model board are described in a journal paper [15].
- Together with Peter Höfner (Data61, CSIRO, Sydney, Australia), H. Garavel set up a model repository (hosted on the Gforge of Inria) to collect and archive formal models of real systems; this infrastructure is used by the series of MARS workshops [0]. The first model deposited in this repository was W. Serwe's description in LOTOS and LNT of an asynchronous circuit implementing the Data Encryption Standard.
- G. Salaün is member of the steering committee of the SEFM (*International Conference on Software Engineering and Formal Methods*) conference series since 2014.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- R. Mateescu was the tool chair of TACAS'2016 (*22th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*), Eindhoven, The Netherlands, April 2–8, 2016.
- G. Salaün was co-chair of SVT-SAC'2016 (the *Software Verification and Testing* track of the *31st ACM Symposium on Applied Computing*), Pisa, Italy, April 4–8, 2016.

9.1.2.2. Member of the Conference Program Committees

- H. Garavel was program committee member of the 6th FMF (*Forum Methodes Formelles*), Toulouse-Grenoble-Saclay, France, January 26, 2016.
- F. Lang was program committee member of GaM'2016 (*Graphs as Models*), Eindhoven, The Netherlands, April 2–3, 2016.
- G. Salaün was program committee member of SOAP-SAC'2016 (the *Service-Oriented Architecture and Programming* track) of SAC'2016, Pisa, Italy, April 4–8, 2016.
- R. Mateescu was program committee member of SPIN'2016 (*23rd International SPIN Symposium on Model Checking of Software*), Eindhoven, The Netherlands, April 7–8, 2016.
- G. Salaün was program committee member of CIEL'2016 (*5ème Conférence en IngénieriE du Logiciel*), Besançon, France, June 7, 2016.
- G. Salaün was program committee member of COMPSAC'2016 (*40th IEEE International Conference on Computers, Software and Applications*), Atlanta, Georgia, USA, June 10–14, 2016.
- G. Salaün was program committee member of WWV'2016 (*12th International Workshop on Automated Specification and Verification of Web Systems*), Porto, Portugal, June 26, 2016.

[0] http://mcc.lip6.fr/models.php
[0] http://www.mars-workshop.org/

- H. Garavel and G. Salaün were program committee members of SEFM'2016 (*14th International Conference on Software Engineering and Formal Methods*), Vienna, Austria, July 4–8, 2016.
- G. Salaün was program committee member of RV'2016 (*16th International Conference on Runtime Verification*), Madrid, Spain, September 23–30, 2016.
- R. Mateescu was program committee member of FMICS-AVoCS'2016 (*International Workshop on Formal Methods for Industrial Critical Systems and Automated Verification of Critical Systems*), Pisa, Italy, September 26–29, 2016.
- H. Garavel was program committee member of HILT'2016 (*Workshop on High Integrity Language Technology*), Pittsburgh, PA, October 6–7, 2016.
- R. Mateescu was program committee member of ICTSS'2016 (*28th International Conference on Testing Software and Systems*), Graz, Austria, October 17–19, 2016.
- G. Salaün was program committee member of FACS'2016 (*13th International Conference on Formal Aspects of Component Software*), Besançon, France, October 19–21, 2016.

9.1.2.3. Reviewer

- G. Barbon was a reviewer for COMPSAC'2016, SVT-SAC'2017, and FSEN'2017 (*7th IPM International Conference on Fundamentals of Software Engineering*), Tehran, Iran, April 26–28, 2017.
- H. Garavel was a reviewer for SPIN'2016.
- F. Lang was a reviewer for FORTE'2016 (*36th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems*), Heraklion, Crete, Greece, June 6–9, 2016.
- R. Mateescu was a reviewer for FACS'2016 and SEFM'2016.
- G. Salaün was a reviewer for DAIS'2016 (*16th IFIP International Conference on Distributed Applications and Interoperable Systems*), Heraklion, Crete, Greece, June 6–9, 2016.
- W. Serwe was a reviewer for SEFM'2016, FMICS-AVoCS'2016, RV'2016, and DATE'2017 (*20th International Conference on Design, Automation and Test in Europe*), Lausanne, Switzerland, March 27–31, 2017.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- H. Garavel is an editorial board member of STTT (*Springer International Journal on Software Tools for Technology Transfer*).

9.1.3.2. Reviewer - Reviewing Activities

- G. Barbon was a reviewer for JSS (*Journal of Systems and Software*).
- H. Garavel was a reviewer for the Mathematical Reviews (MathSciNet) of the American Mathematical Society.
- F. Lang was a reviewer for STTT.
- R. Mateescu was a reviewer for Acta Informatica and STTT.
- G. Salaün was a reviewer for IJCIS (*International Journal of Cooperative Information Systems*), JLAMP (*Journal of Logic and Algebraic Methods in Programming*), IEEE TSE (*Transactions on Software Engineering*), and TSI (*Technique et Science Informatiques*).
- W. Serwe was a reviewer for SPE (*Journal on Software: Practice and Experience*) and STTT.

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, the PMC model checker, and the DLC compiler.

In 2016, the main facts are the following:

- We prepared and distributed twelve successive versions (2016-a to 2016-l) of CADP.
- A new version 2.8 of TRAIAN was released on February 29, 2016.
- We were requested to grant CADP licenses for 507 different computers in the world.

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

By the end of December 2016, the CADP forum [0], opened in 2007 for discussions regarding the CADP toolbox, had over 389 registered users and over 1769 messages had been exchanged.

Also, for the 2016 edition of the Model Checking Contest, we provided four families of models (totalling 62 Nested-Unit Petri Nets) derived from our LNT models. A journal article presenting the achievements of the Model Checking Contest since its origins has been published [15].

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:

- An approach for specifying formally the composition of Web services [27]
- The Vercors integrated environment for verifying and running distributed components [43], [46]
- The PN2MC tool for modeling and verifying RTCP-nets [53]
- The Alvis tool for designing hierarchical communication diagrams [54]
- The IDCM tool for designing and integrating complex systems [48], [47]
- The Availability Analyzer tool for software architecture decomposition alternatives [55]

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

- Formal specification and verification of TCP extended with the Window Scale Option [49]
- Performance evaluation of concurrent data structures [56]
- Heuristic search for equivalence checking [31]
- Using formal models to cross check an implementation [52]
- Proving linearizability via branching bisimulation [57]
- Computing maximal weak and other bisimulations [28]
- Verification methodologies for fault-tolerant Network-on-Chip systems [58]

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. Invited Talks

- H. Garavel gave a talk entitled "*Process Calculi: Towards the Great Unification*" on January 12, 2016 at the Formal Methods seminar of Inria Grenoble.
- R. Mateescu gave a talk entitled "*On-the-Fly Verification for Extended Action-Based Temporal Logics*" on March 3rd, 2016 at IST Graz, Austria.
- H. Garavel was a guest speaker at the 9th German national D-CON meeting that took place in Saarbrücken, Germany, on March 7–8, 2016, where he gave a talk entitled "*Nested-Unit Petri Nets*".
- G. Salaün gave a talk entitled "*Automated Verification of Asynchronously Communicating Systems*" on March 15, 2016 at the LORIA laboratory, Nancy, France.
- H. Garavel gave a talk entitled "*On the Simplest Way to Build Integers from Naturals*" on April 28, 2016 at Saarland University, Germany.

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

- G. Barbon gave a talk entitled "*Debugging Concurrent Programs using Model Checking and Mining Techniques*" at MOVEP'2016 (*12th Summer School on Modelling and Verification of Parallel Processes*) that took place in Genova, Italy, on June 17–July 1, 2016.
- H. Garavel gave a talk entitled "*On the Most Suitable Axiomatization of Signed Integers Using Free Constructors*" during WADT'2016 (*23rd International Workshop on Algebraic Development Techniques*) that took place in Gregynog, Wales, UK, on September 21–24, 2016.
- H. Garavel gave two talks entitled "*Term Rewrite Systems and the Definition of Signed Integers*" and "*Benchmarking Implementations of Conditional Term Rewrite Systems*" on September 30, 2016 at the LSV laboratory, Cachan, France.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

CONVECS is a host team for MOSIG [0] (*Master of Science in Informatics at Grenoble*), the international master programme in computer science, common to Grenoble INP and Université Grenoble Alpes.

In 2016, we carried out the following teaching activities:

- H. Garavel, together with Laurence Pierre (TIMA, Grenoble), created a new curriculum HECS [0] ("*High-confidence Embedded and Cyberphysical Systems*") for 2nd-year MOSIG students. This curriculum opened for the first time in September 2016.
- F. Lang, R. Mateescu, G. Salaün, and W. Serwe gave lectures on models for concurrency, temporal logics, equivalences, formal languages and verification (36 hours) as part of the MOSIG/HECS-2 course ("*Modeling and Analysis of Concurrent Systems*") led by G. Salaün.
- H. Garavel gave lectures on probabilistic models, stochastic models, and static/dynamic fault trees (6 hours) as part of the MOSIG/HECS-3 course ("*Performance and quantitative properties*") led by Goran Frehse (Verimag).
- H. Garavel gave lectures on the synchronous languages Lustre and SCADE, and on model-driven engineering (7.5 hours) as part of the MOSIG/HECS-4 course ("*Industrial processes for high-confidence design*") led by Laurence Pierre (TIMA).
- G. Salaün was co-responsible of the ISI (*Ingéniérie des Systèmes d'Information*) department of ENSIMAG ("*École Nationale Supérieure d'Informatique et de Mathématiques Appliquées*", Grenoble INP) from September 1, 2011 until August 31st, 2016.
- G. Salaün is Professor at Université Grenoble Alpes since September 1st, 2016, and teaches algorithmics, programming, and Web development at the MMI department of IUT1. He is also headmaster of the SMIN professional licence (L3, 3rd year of university), 192 hours.
- W. Serwe supervised a group of six teams in the context of the "*projet Génie Logiciel*" (55 hours "*équivalent TD*", consisting in 16.5 hours of lectures, plus supervision and evaluation).
- F. Lang gave a lecture on formal methods (9 hours "*équivalent TD*") in the framework of the software engineering course given to the first year students of MOSIG.
- F. Lang gave a lecture on "*Modélisation et vérification de systèmes concurrents et temps-réel*" (27 hours "*équivalent TD*") to the third year computer science engineering students of ENSIMAG.
- G. Barbon gave a lecture on "*Théorie des Langages 1*" at ENSIMAG (18 hours "*équivalent TD*").

[0] http://mosig.imag.fr
[0] http://hecs.imag.fr

9.2.2. Supervision

- Fatma Jebali, "*A Formal Framework for Modelling and Verifying Globally Asynchronous Locally Synchronous Systems*", Université Grenoble Alpes, September 12, 2016, F. Lang and R. Mateescu
- PhD in progress: G. Barbon, "*Debugging Concurrent Programs using Model Checking and Mining Techniques*", Université Grenoble Alpes, since October 2015, G. Salaün and V. Leroy
- PhD in progress: L. Marsso, "*Formal Methods for Testing Networks of Controllers*", Université Grenoble Alpes, since October 2016, R. Mateescu, W. Serwe, I. Parissis, and Ch. Deleuze
- PhD in progress: U. Ozeer, "*Autonomous Resilience of Applications in a Largely Distributed Cloud Environment*", Université Grenoble Alpes, since November 2016, X. Etchevers, G. Salaün, F.-G. Ottogalli, and J.-M. Vincent

9.2.3. Juries

- R. Mateescu was reviewer of Oleksandra Kulankhina's PhD thesis, entitled "*A Framework for Rigorous Development of Distributed Components: Formalisation and Tools*", defended at University of Nice Sophia-Antipolis on October 14, 2016.
- G. Salaün was reviewer of Guillaume Verdier's PhD Thesis, entitled "*Variants of Acceptance Specifications for Modular System Design*", defended at University of Toulouse on March 29, 2016.

9.3. Popularization

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

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

9.4. Miscellaneous Activities

H. Garavel was a member of the 2016 Inria selection committee for hiring research officers (*chargés de recherche*).

In 2016, H. Garavel was appointed to the Executive Commission in charge of International Relations at COMUE University Grenoble Alpes.

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

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

R. Mateescu is a member of the "*Comité d'orientation scientifique*" for Inria Grenoble – Rhône-Alpes.

R. Mateescu is a member of the "*Bureau*" of the LIG laboratory.

G. Salaün was an elected member of the council of the LIG laboratory until August 31, 2016.

G. Salaün is a member of the Scientific Committee of the PCS action of the PERSYVAL Labex.

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

W. Serwe is (together with Laurent Lefèvre from the AVALON Inria project-team) correspondent in charge of the 2016 Inria activity reports at Inria Grenoble – Rhône-Alpes.

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

HYCOMES Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Member of the Conference Program Committees

Benoî Caillaud has served on the program committee of ACSD 2016 (http://acsd2016.mat.umk.pl), a conference on the applications of concurrency in system design. He is a member of the steering committe of ACSD since 2006.

9.1.1.2. Reviewer

Benoît Caillaud has reviewed papers submitted to the ACSD 2016 and ACC 2016 conferences.

Khalil Ghorbal reviewed two regular research papers for the Hybrid Systems: Computation and Control Conference.

Khalil Ghorbal reviewed two journal papers for the IEEE Transactions on Automatic Control.

Khalil Ghorbal reviewed a journal paper for the Computer Journal (Oxford Journals, Science and Mathematics).

Khalil Ghorbal reviewed a journal paper for the Information and Computation journal (Elsevier).

9.1.2. Invited Talks

Benoît Caillaud has given an invited talk on *Time Domains in Hybrid Systems Modeling* at the SHARC 2016 workshop and ALROB meetingthat took place in Brest in June 2016 (http://lab-sticc.univ-brest.fr/~goulven/sharc2016/program/index.html).

In May 13, 2016, Khalil Ghorbal gave an invited talk about the invariant generation for polynomial ordinary differential equations during the Effective Algebraic Geometry Seminar, IRMAR, Rennes, France.

In May 23, 2016, Ayman Aljarbouh presented a talk at the Embassy of Sweden in Tokyo for the first Japanese Modelica Conference (MODELICA2016), May 23-24, 2016, Tokyo, JAPAN.

In July 2016, Ayman Aljarbouh presented a poster during the French-American Doctoral Exchange Seminar (FADEx) 2016: Systèmes Cyber-Physiques, July 04-08, 2016, Grenoble, FRANCE.

In November, 5-12, Albert Benveniste was invited at the Systems Research Center, a center of excellence of the University of Maryland at College Park, USA.

9.1.3. Research Administration

Benoît Caillaud is head of the *Languages and Software Engineering* department of IRISA (http://www.irisa.fr/en/departments/d4-language-and-software-engineering). He has been in charge of presenting the departement during the evaluation seminar of IRISA by HCERES in January 2016.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Benoît Caillaud is teaching with Marc Pouzet a first year master degree course on *hybrid systems modeling*. The course is open to the students registered to the computer science research and innovation curriculum of the university of Rennes 1 and ENS Rennes, France.

Master : Khalil Ghorbal was "Chargé de TD" (20h Eq TD) for the "Analyse et Conception Formelles" module open for students registered to the computer science master degree of the university of Rennes 1 and ENS Rennes, France.

9.2.2. Supervision

PhD in progress : Ayman Aljarbouh, *Accelerated Simulation of Hybrid Systems*, started january 2014, supervised by Benoît Caillaud. Ayman Aljarbouh is expected to defend his PhD in MArch 2017.

9.2.3. Juries

Khalil Ghorbal was reviewer in the PhD defense committee of Sameh Mohamed, "Une Méthode Topologique pour la Recherche d'Ensembles Invariants de Systèmes Continus et á Commutation", defended in October 17th, 2016, Univ. Paris Saclay (ENS Cachan).

MUTANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Selection

8.1.1.1. Member of the Conference Program Committees

Jean-Louis Giavitto has participated in the program committee of the 42st International Computer Music Conference (ICMC), the 10th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO 2016), the Digital Entertainment Technologies and Arts(DETA) of GECCO-2016, the 15th International Conference on the Synthesis and Simulation of Living Systems (ALIFE XV) and the 2nd International Conference on Technologies for Music Notation and Representation (TENOR 2016).

Florent Jacquemard has been involved in the Program Committees of the 2d International Conference on Technologies for Music Notation and Representation (TENOR 2016), the 8th International Symposium on Symbolic Computation in Software (SCSS 2017), the National Conference *Journées d'Informatique Musicale* (JIM 2016), and the special issue of the journal Information and Computation for the 10th International Conference on Language and Automata Theory and Applications (LATA 2016).

8.1.1.2. Member of the Editorial Boards

Jean-Louis Giavitto is associate redactor (former redactor-in-chief) of TSI (Technique et Science Informatiques) published by Lavoisier. He has coorganized with Antoine Spicher (Univ. Paris Est), Stefan Dulman (Univ. Twente) and Mirko Viroli (Univ. of Milano) a special issue of *The Knowledge Engineering Review* on Spatial Computing published in november 2016.

8.1.1.3. Reviewer - Reviewing Activities

The members of the team contributed as reviewers for the journal Information and Computation, IEEE Transactions on Multimedia, IEEE Transactions on Audio and Speech Signal Processing, ACM Transactions on Intelligent Systems, Theoretical Computer Science, IEEE ICASSP, ICMC, SMC, Formal Methods, LATA and more...

8.1.2. Invited Talks

Jean-Louis Giavitto was invited to the seminar @SystemX at Saclay.

Florent Jacquemard gave an invited talk at the 5th International Workshop on Confluence (IWC 2016), hosted by Innsbruck University Center at Obergurgl, Austria [19].

8.1.3. Leadership within the Scientific Community

Jean-Louis Giavitto was a member of the Prix de thèse du GDR GPL as well as a member of the Faust Award 2016 (the Faust Open-Source Software Competition is intended to promote innovative high-quality free audio software developed with the Faust programming language, as well as development tools build around the Faust compiler itself).

8.1.4. Scientific Expertise

Jean-Louis Giavitto is in scientific board of the GDR GPL (Genie de la programmation et du logiciel). He is also a reviewer for FET projects for the UC.

8.2. Teaching - Supervision - Juries

8.2.1. Supervision

- PhD defended: José Echeveste, *Accorder le temps de la machine et celui du musicien*, started in October 2011, supervisor: Arshia Cont and Jean-Louis Giavitto.
- PhD defended (November 2016): Clément Poncelet, Formal methods for analyzing human-machine interaction in complex timed scenario. Started in October 2013, supervisor: Florent Jacquemard.
- PhD defended (December 2016): Philippe Cuvillier, Probabilistic Decoding of strongly-timed events in realtime, supervisor: Arshia Cont.
- PhD in progress: Julia Blondeau, *Espaces compositionnels et temps multiples : de la relation forme/matériauq (thèse en art)*, supervisor: Jean-Louis Giavitto, co-director Dominique Pradelle (Philosophy, Sorbonne), started October 2015.
- PhD in progress: Maxim Sirbu, Online Interaction via Machine Listening. Supervisors: Arshia Cont (MuTant) and Mathieu Lagrange (IrCyNN), started October 2015.
- PhD in progress: Pierre Donat-Bouillud, Modeling, analysis and execution of cyber-temporal systems. Supervisor: Florent Jacquemard, co-director: Jean-Louis Giavitto, started October 2016.

8.2.2. Juries

Jean-Louis Giavitto was Chairman of the jury of Clément Poncelet. He was reviewer of the PhD thesis of Jaime Arias (University of Bordeaux, Sémantique Formelle et Vérification Automatique de Scénarios Hiérarchiques Multimédia avec des Choix Interactifs), and examiner of the PhD of Mattia Bergomi (Università di Milano and UPMC, Dynamical and Topological Tools for (Modern) Music Analysis).

Florent Jacquemard was reviewer of the PhD thesis of Etienne Dubourg (University of Bordeaux, Contributions to the theory of tile languages). He is reviewer of the PhD thesis of Nicolas Guiomard-Kagan (Université de Picardie Jules Verne, *Traitement de la polyphonie pour l'analyse informatique de partitions musicales*). He has been examiner of the PhD of Emil-Mircea Andriescu (UPMC, MiMove, Dynamic Data Adaptation for the Synthesis and Deployment of Protocol Mediators) and examiner of the PhD of Carles Creus Lo´pez (UPC Barcelona, Tree Automata with Constraints and Tree Homomorphisms).

PARKAS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Albert Cohen is the General Chair of PLDI 2017

9.1.1.2. Member of the Conference Program Committees

- Timothy Bourke was a member of the PC of EMSOFT 2016.
- Francesco Zappa Nardelli was a member of the PC of POPL 2017.
- Francesco Zappa Nardelli will be a member of the PC of ECOOP 2017.
- Albert Cohen was a PC member of ASPLOS, PACT, PPoPP, CGO, PLDI.

9.1.1.3. Reviewer

- Timothy Bourke was a reviewer for FM 2016 (Int. Symposium on Formal Methods).

9.1.2. Journal

9.1.2.1. Member of the Editorial Boards

- Albert Cohen is an Associate Editor of ACM TACO.

9.1.2.2. Reviewer - Reviewing Activities

- Timothy Bourke was a reviewer for IEEE Embedded Systems Letters, ACM Transactions on Embedded Computing Systems, and IEEE Transactions on Software Engineering.

9.1.3. Invited Talks

- April, T. Bourke presented “Towards the verified compilation of Lustre” in the Gallium seminar series in Paris, France.
- December, T. Bourke presented “Verifying a Lustre Compiler (Part 1)” at the SYNCHRON workshop in Bamberg, Germany.
- November, F. Zappa Nardelli presented “Shared Memory Concurrency and Compiler Optimisations” at IMDEA, Madrid, Spain.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: F. Zappa Nardelli: “A Programmer’s introduction to Computer Architectures and Operating Systems" (M1), 45h, École Polytechnique, France

Master: A. Cohen & F. Zappa Nardelli, “Semantics, languages and algorithms for multicore programming", Lecture, 9h+12h, M2, MPRI: Ecole normale supeérieure and Université Paris Diderot, France

Licence: F. Zappa Nardelli: “Conception et analyse d’algorithmes" (L3), PCs, 32h, E´cole Polytechnique, France

Master : M. Pouzet & T. Bourke: “Synchronous Systems” (M2), Lectures and TDs, MPRI, France

Master: T. Bourke participated in reviewing the M1 internships of students at the ENS, France.

Licence : M. Pouzet & T. Bourke: “Operating Systems” (L3), Lectures and TDs, ENS, France.

Licence : T. Bourke, “Digital Systems” (L3), Lectures and TDs, ENS, France

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

9.2.2. Supervision

PhD in progress : Ulyssse Beaugnon, 2nd year, supervised by A. Cohen and M. Pouzet.

PhD in progress : Chandan Reddy, 2nd year, supervised by A. Cohen.

PhD in progress : Jie Zhao, 2nd year, supervised by A. Cohen.

PhD in progress : Guillaume Baudart, 3rd year, supervised by T. Bourke and M. Pouzet. This thesis will be defended in March.

PhD in progress : Lélio Brun, 1st year, supervised by T. Bourke and M. Pouzet.

PhD in progress : Robin Morisset, 3rd year, supervised by F. Zappa Nardelli. This thesis will be defended in April 2017.

9.2.3. Juries

Francesco Zappa Nardelli was an external reviewer of the PhD thesis of Carl Leonardsson, Uppsala University, Sweden.

Francesco Zappa Nardelli was a jury member of the PhD thesis of Nhat Minh Lê, ENS, Paris, France.

Timothy Bourke was an external reviewer of the masters thesis of Shruti Saini, The University of the South Pacific.

POSET Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- D. Janin, General Chair of ACM Workshop on Functional Art, Music, Modeling and Design (FARM), Nara (Japan), associated with ICFP,

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- D. Janin, PC Chair of Journées d'Informatique Musicale (JIM 2015), Albi (France),

10.1.2.2. Member of the Conference Program Committees

- M. Desainte-Catherine, PC member of Journées d'Informatique Musicale (JIM 2015), Albi (France),

10.1.2.3. Reviewer

Members of the project are yearly reviewers for a number of international conferences including LICS, ICALP, STACS, MFCS, FST&TCS, in theoretical computer science, and ICMC, SMC, NIME, FARM, TENOR, JIM in computer music.

10.1.3. Journal

10.1.3.1. Member of the editorial boards

- S. Salvati is editor of the Journal of Logic Language and Information (JoLLI); since the end of 2015, he has been promoted as Editor in Chief,
- M. Desainte-Catherine is editor of the Revue francophone d'informatique musicale (RFIM).

10.1.3.2. Reviewer - Reviewing activities

Members of the project are regular reviewers for a number of international journal including ACM Computers In Entertainment (CIE), Journal of New Music Research (JNMR), Journal of Logic Language and Information (JoLLI), Revue francophone d'informatique musicale (RFIM), Discrete Mathematics &Theoretical Computer Science (DMTCS), International Journal of Foundations of Computer Science (IJFCS), Information & Computation (I&C) ...

10.1.4. Leadership within the Scientific Community

- M. Desainte-Catherine is president of the Association Française d'Informatique Musicale (AFIM)
- S. Salvati is the secretary of the Foundation for Logic Language and Information (FoLLI).

10.1.5. Research Administration

- M. Desainte-Catherine, directrice adjointe du LaBRI,
- M. Desainte-Catherine, directrice scientifique et administrative du SCRIME,
- M. Desainte-Catherine, responsable du thème SI de l'équipe image et son du LaBRI,
- D. Janin, membre commission recherche Bordeaux INP/ENSEIRB-MATMECA.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Myriam Desainte-Catherine, *Programmation fonctionnelle*, 44 h, L3, Software Engineering department, Bordeaux INP, France,
Licence: Myriam Desainte-Catherine, *Projet d'algorithmique et de programmation*, 25 h, L3, Software Engineering department, Bordeaux INP, France,
Licence: Anne Dicky, *Algorithmique des graphes*, 30 h, L3, Computer Science Departement, Paris VI University, Vietnam,
Licence: Anne Dicky, *Probabilités et combinatoire*, 75 h, L3, Computer Science Departement, Bordeaux University, France,
Licence: Anne Dicky, *Algorithmique et structures de données*, 50h, L2, Computer Science Departement, Bordeaux University, France,
Licence: Anne Dicky, *Fondamentaux pour les mathématiques et l'informatique*, 35 h, L1, Computer Science Departement, Bordeaux University, France,
Master: Sylvain Salvati, *Logique*, 12h, M1, Computer Science Departement, Bordeaux University, France,
Licence: David Janin, *Projet d'algorithmique et de programmation*, 25 h, L3, Software Engineering department, Bordeaux INP, France,
Licence: Sylvain Salvati, *Analyse syntaxique et projet de programmation 3*, 37,5 h, niveau L3, Computer Science Departement, Bordeaux University, France,
Master: Myriam Desainte-Catherine, *Compilation*, 14 h, M1, Software Engineering department, Bordeaux INP, France,
Master: Myriam Desainte-Catherine, *Projet de Génie Logiciel*, 25 h, M1, Software Engineering department, Bordeaux INP, France,
Master: Myriam Desainte-Catherine, *Informatique musicale contrôle et composition*, 25 h, M2, Software Engineering department, Bordeaux INP, France,
Master: Anne Dicky, *Recherche operationelle*, 70 h, M1, Computer Science Departement, Bordeaux University, France,
Master: David Janin, *Projet de Génie Logiciel*, 25 h, M1, Software Engineering department, Bordeaux INP, France,
Master: David Janin, *Compilation*, 20 h, M1, Network and System Engineering department (RSI), Bordeaux INP, France,
Master: David Janin, *Tutorat*, 15 h, M1, M2, Network and System Engineering department (RSI), Bordeaux INP, France,
Doctorat: Sylvain Salvati, *Initiation à CoQ*, 12 h, Ecole Doctorale Mathématique et Informatique, Bordeaux University, France.

10.2.2. Supervision

PhD : Etienne Dubourg, "Contribution à la théorie des langages de tuiles", defended in July 2016, supervised by D. Janin
PhD in progress : Pauline Mouawad, "Analyse et modélisation de l'émotion musicale"', started in september 2012, supervised by M. Desainte-Catherine,
PhD in progress : Jean-Michaël Célérier, "Outils d'écriture spatiale pour les partitions interactives", started in january 2015, supervised by M. Desainte-Catherine,
PhD in progress : Simon Archipoff, "Modélisation et programmation tuilée réactive", started in september 2015, supervised by D. Janin,

10.2.3. Juries

- D. Janin, member of the PhD jury of Clément Poncelet, "Model-Based Testing Real-Time and Interactive Music Systems", Université Paris VI / IRCAM, November 2016,

10.3. Popularization

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

SPADES Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of organizing committees

- Sophie Quinton was artifact evaluation chair of the 24th International Conference on Real-Time Networks and Systems (RTNS'16).
- Sophie Quinton was demo chair of the 22nd IEEE Real-Time Embedded Technology & Applications Symposium (RTAS'16)
- Sophie Quinton was co-chair of the 1st Tutorial on Tools for Real-Time Systems (TuToR'16), held as a satellite event of CPSWeek'16. http://tutor2016.inria.fr/
- Sophie Quinton was co-organizer of the 1st Workshop on Collaboration of Academia and Industry for Real World Embedded Systems (CAIRES'16), held as a satellite event of ESWeek'16. http://caires2016.inria.fr/

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- Gregor Gössler was co-chair of the 1st international Workshop on Causal Reasoning for Embedded and safety-critical Systems Technologies (CREST'16) [22], held as a satellite event of ETAPS'16. http://crest2016.inria.fr
- Sophie Quinton was co-chair of the 7th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS'16), held as a satellite event of ECRTS'16. http://waters2016.inria.fr

9.1.2.2. Member of conference program committees

- Pascal Fradet served in the program committee of the 15th International Conference on Modularity (MODULARITY'16).
- Alain Girault served in the program committees of the International Conference on Design and Test in Europe (DATE'16), the Embedded Software conference (EMSOFT'16), and the International Symposium on Industrial Embedded Systems (SIES'16).
- Sophie Quinton served in the program committees of the 28th Euromicro Conference on Real-Time Systems (ECRTS'16), the 24th International Conference on Real-Time Networks and Systems (RTNS'16), the 4th International Workshop on Mixed Criticality Systems (WMC'16), the 10th Junior Researcher Workshop on Real-Time Computing (JRWRTC'16), and in the artifact evaluation committees of ECRTS'16 and the IEEE Real-Time Systems Symposium (RTSS'16).
- Jean-Bernard Stefani served on the program committees of the 36th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems (FORTE) and the 8th Conference on Reversible Computation.

9.1.2.3. Reviewer

- Alain Girault reviewed an article for ECRTS'16.
- Gregor Gössler reviewed articles for EMSOFT'16, FACS'16, and RTNS'16.
- Xavier Nicollin reviewed an article for SIES'16.
- Sophie Quinton reviewed articles for EMSOFT'16 and DATE'17.

9.1.3. Journal

9.1.3.1. Member of the editorial boards

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

9.1.3.2. Reviewer - Reviewing activities

- Alain Girault reviewed articles for ACM TECS, Parallel Computing, Embedded Systems Letters, and Microprocessors and Microsystems.
- Gregor Gössler reviewed articles for Formal Methods in System Design (FMSD) and IEEE Transactions on Automatic Control (TAC).
- Jean-Bernard Stefani reviewed articles for Theoretical Computer Science (TCS) and Science of Computer Programming (SCP).

9.1.4. Research administration

- Pascal Fradet is head of the committee for doctoral studies ("Responsable du comité des études doctorales") of the INRIA Grenoble – Rhône-Alpes research center and local correspondent for the young researchers INRIA mission (mission jeunes chercheurs).
- Alain Girault is Vice Chair of the INRIA Evaluation Committee. As such, he co-organizes in particular the evaluation seminars of the INRIA teams (twice a year) and all the juries for the hiring and promotion of INRIA's researchers (CR2, CR1, DR2, DR1, and DR0).
- Jean-Bernard Stefani is Head of science of the INRIA Grenoble – Rhône-Alpes research center. As such, he manages with the research center director all aspects of the scientific life of the research center (creation of the research teams and their evaluation by international panels, scientific relationships with our academic and industrial partners, hiring of the new junior researchers, ...).
- Jean-Bernard Stefani is co-director of I/O LAB, the joint research laboratory with Orange Lab.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Pascal Fradet, Théorie des Langages 1 & 2, 36 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Gregor Gössler, Théorie des Langages 2, 36 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Master : Xavier Nicollin, Sémantique et Analyse des Programmes, 11,25 HeqTD, niveau M1, Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Théorie des Langages 2, 36 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Bases de la Programmation Impérative, 66 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Sophie Quinton, Théorie des Langages 2, 18 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Master : Jean-Bernard Stefani, Formal Aspects of Component Software, 9h, MOSIG, Univ. Grenoble Alpes, France

Master : Sophie Quinton, Performance and Quantitative Properties, 6h, MOSIG, Univ. Grenoble Alpes, France

9.2.2. Supervision

- PhD: Yoann Geoffroy, "A general trace-based causality framework for component-based systems", Univ. Grenoble Alpes, defended on December 7th 2016, advised by Gregor Gössler.
- PhD in progress: Sihem Cherrared, "Fault Management in Multi-Tenant Programmable Networks", Univ. Rennes 1, since October 2016, co-advised by Eric Fabre and Gregor Gössler.
- PhD in progress: Christophe Prévot, "Early Performance assessment for evolving and variable Cyber-Physical Systems", Univ. Grenoble Alpes, since November 2015, co-advised by Alain Girault and Sophie Quinton.
- PhD in progress: Xiaojie Guo, "Formal Proofs for the Analysis of Real-Time Systems in Coq", Univ. Grenoble Alpes, since December 2016, co-advised by Pascal Fradet, Jean-François Monin, and Sophie Quinton.
- PhD in progress: Stephan Plassart, "On-line optimization in dynamic real-time systems", Univ. Grenoble Alpes, since September 2016, co-advised by Alain Girault and Bruno Gaujal.

9.2.3. Juries

- Alain Girault was president of the HDR jury of Goran Frehse (Univ. Grenoble Alpes).
- Sophie Quinton was member of the PhD jury of Houssam Zahaf (U. Lille).
- Jean-Bernard Stefani was president of the HDR jury of Tom Hirschowitz (U. Savoie).

9.3. Popularization

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

TEA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

Jean-Pierre Talpin served as General Chair and Finance Chair of the 14th. ACM-IEEE Conference on Methods and Models for System Design (MEMOCODE'16, IIT Kanpur, October 18-20.).

10.1.1.2. Member of the organizing committees

Jean-Pierre Talpin and Vania Joloboff co-organized the Shonan workshop on "Architecture-Centric Modeling, Analysis, and Verification of Cyber-Physical Systems" in collaboration with Toyota ITC and Denso, March 21-24.

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

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

Jean-Pierre Talpin served the program committee of:

- ACVI'16, 3rd. Workshop on Architecture Centric Virtual Integration
- HLDVT'16, 18th. IEEE International High-Level Design Validation and Test Workshop
- ICESS'16, 13th. IEEE International Conference on Embedded Software and Systems
- IDEA'16, 2nd. International Workshop Integrating Data-flow, Embedded computing and Architecture
- LCTES'16, 19th. ACM SIGPLAN-SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems
- MEMOCODE'16, 14th. ACM-IEEE Conference on Methods and Models for System Design
- SAC'16, 31st. ACM SIGAPP Symposium on Applied Computing
- SCOPES'16, 19th. International Workshop on Software and Compilers for Embedded Systems
- TASE'16, 10th. Theoretical Aspects of Software Engineering Conference

10.1.3. Journal

10.1.3.1. Member of the editorial boards

Jean-Pierre Talpin is Associate Editor with the ACM Transactions for Embedded Computing Systems (TECS), with the Springer journal on Frontiers of Computer Science (FCS) and with the EURASIP journal of embedded systems (JES).

10.1.3.2. reviewer

Jean-Pierre Talpin reviewed articles for Acta Informatica.

Thierry Gautier reviewed for Frontiers of Computer Science.

10.2. Teaching - Supervision - Juries

10.2.1. Invited talks

Vania Joloboff gave a talk in the series of the Distinguished Lecturers of the Computer Science and Engineering department at UC San Diego.

Jean-Pierre Talpin gave an invited presentation at the APAC 2016 Summit on Robotics at the HKSTP in Hong Kong https://www.apacinnosummit.net.

10.2.2. Supervision

Vania Joloboff supervised work of Master student Daian Yue that was selected in the joint program between ENS Rennes and ECNU.

Jean-Pierre Talpin is the supervisor of Simon Lunel's thesis on "*Timed contract algebras for correct by construction real-time system design*".

10.2.3. Juries

Jean-Pierre Talpin served as examiner for the Ph.D. Thesis defense of Fatma Jebali on "Formal Framework for modeling and Verifying Globally Asynchronous Locally Synchronous Systems", September 12., in Grenoble.

Jean-Pierre Talpin served as referee for the PhD. Thesis Defence of Amani Khecharem on "Une approche de méta-modélisation pour la représentation multi-vues des architectures hétérogènes embarqués", May 3., in Sophia Antipolis.

ANTIQUE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Jérôme Feret is a member of the editorial board of the Frontiers in Genetics journal and the Open Journal of Modeling and Simulation.

9.1.1.2. Member of the Organizing Committees

Jérôme Feret organized the 40th of Abstract Interpretation at POPL2017 January 21, 2017, Paris, France (co-organizer).

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Xavier Rival was chair of Static Analysis Symposium SAS 2016, Edinburgh.

Jérôme Feret co-chaired the fifteenth Conference on Computational Methods in Systems Biology - CMSB 2017, September 27–29, 2017, Darmstadt, Germany.

9.1.2.2. Member of the Conference Program Committees

Vincent Danos served on the PC of Computational Methods in Systems Biology, CMSB'16, Cambridge and Complexis'17.

Xavier Rival served on the PC of the 26th European Symposium on Programming (ESOP 2017).

Cezara Drăgoi served on the PC of

- 28th International Conference on Computer-Aided Verification (ERC), CAV 2016,
- 37th INTERNATIONAL CONFERENCE ON APPLICATIONS AND THEORY OF PETRI NETS AND CONCURRENCY, ACSD 2016,
- 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2017,
- 18th International Conference on Verification, Model Checking, and Abstract Interpretation, VMCAI 2017,
- ACM SIGPLAN Symposium on Programming Language Design & Implementation, PLDI 2017.

Jérôme Feret served on the PC of

- the 8th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies - BIOTECHNO 2016,
- the 26th International Symposium on Logic-Based Program Synthesis and transformation - LOPSTR 2016,
- the 23rd Static Analysis Symposium Sept 8-10 2016, Edinburgh,
- 7th International Workshop on Static Analysis and Systems Biology - SASB 2016,
- 14th International Conference on Computational Methods in Systems Biology - CMSB 2016 Sept 21-23 2016, Cambridge, UK,
- Fourth International Conference on Tools and Methods for Program Analysis - TMPA 2017 March 3–4, 2017, Moscow, Russia, JOBIM 2017 July 2-6 2017, Lille, France.

9.1.2.3. Reviewer

Vincent Danos was a reviewer for the 19th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS) 2017, the 26th European Symposium on Programming (ESOP 2017) 2017, LMCS, MSCS.

Cezara Drăgoi was a reviewer for 19th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS) 2017, the 27th International Conference on Concurrency Theory CONCUR 2016, and the 26th European Symposium on Programming (ESOP 2017) 2017.

Xavier Rival was a reviewer for 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2017 and ACM SIGPLAN Symposium on Programming Language Design & Implementation, PLDI 2017.

Jérôme Feret was a reviewer for the 17th International Conference on Verification, Model Checking, and Abstract Interpretation, VMCAI 2016, the 27th International Conference on Concurrency Theory CONCUR 2016, the 43rd International Colloquium on Automata, Languages and Programming 2016, the 31st ACM/IEEE Symposium on Logic in Computer Science, LICS 2016.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Jérôme Feret is a member of the editorial board of the Frontiers in Genetics journal and the Open Journal of Modeling and Simulation .

9.1.3.2. Reviewer - Reviewing Activities

Xavier Rival was a reviewer for ACM Transactions on Programming Languages and Systems TOPLAS.

Jerome Feret was a reviewer for Theoretical Computer Science 2016.

9.1.4. Invited Talks

Jérôme Feret gave “An overview of the Astrée/AstréeA analyzer. " at Journées scientifiques Inria Rennes, 20-22 june 2016 and at the workshop « Verified Trustworthy Software Systems » Imperial College, 6-7 April 2016.

Vincent Danos talked about ‘Residence: Simons Institute Program Logical Structures and Computations" at CONCUR 2016, Quebec, Aug 25-2 and at Berkeley, Aug 17-Dec 16. He also gave invited talks at SysMod SIG 2016, ISMB, Orlando, Jul 9, Xenobiology 2, XB2, May 24-26, Berlin, IPM Formal Methods Day, Teheran, Jan 10.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence :

- Xavier Rival, “Semantics and Application to Verification",20h, Undergraduate course (L3), at Ecole Normale Supérieure
- Xavier Rival, “Introduction to Static Analysis", 8h, Course at Ecole des Mines de Paris, L3
- Cezara Drăgoi, “Programation concurrente et distribuée", Ecole Politechnique, L2
- Cezara Drăgoi, “Les principes des langages de programmation", Ecole Politechnique, L1
- Jérôme Feret, and Cezara Drăgoi, Mathematics, 40h, L1, FDV Bachelor program (Frontiers in Life Sciences (FdV)), Université Paris-Descartes, France.

Master :

- Vincent, Disruptive technologies and public policies, MSc Public affairs, Sciences Po, France.

- Xavier Rival, Protocol Safety and Verification, Master Course (M2) in the Advanced Communication Networks Master (12h hours), at Polytechnique and Ecole Nationale Supérieure des Telecoms
- Xavier Rival, “Verification" Lab Course at Ecole Polytechnique (M1, 20h)
- Vindent Danos and Jérôme Feret (with Jean Krivine), Computational Biology, 24h, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.
- Cezara Drăgoi, 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.

Doctorat : Jérôme Feret, “Interprétation abstraite de modèles de voies de signalisation intracellulaire ", Lectures (3 hours) in the summer school “Modélisation Formelle de Réseaux de Régulation Biologique”, Porquerolles, June 2016 France.

9.2.2. Juries

Jérôme Feret was a member of the recruitment committee for an assistant professor in Paris-Diderot University 2016.

Vincent Danos was examiner and reviewer for the HDR of Sylvain Soliman (Ecole Polytechnique, 7th of December 2016).

CELTIQUE Project-Team

6. Dissemination

6.1. Promoting Scientific Activities

6.1.1. Scientific Events Organisation

6.1.1.1. General Chair, Scientific Chair

- PLMW@SPLASH 2016 (Programming Languages Mentoring Workshop) was chaired by Sandrine Blazy and Ulrik Prag-Schultz
- CoqPL 2017 (International Workshop on Coq for PL) was chaired by Sandrine Blazy and Emilio Jesus Gallego Arias

6.1.1.2. Member of the Organizing Committees

- JFLA 2016 (Journées Francophones des Langages Applicatifs) was locally organized by Julien Signoles and Alan Schmitt

6.1.2. Scientific Events Selection

6.1.2.1. Chair of Conference Program Committees

- VSTTE 2016 (Verified Software: Theories, Tools, and Experiments) was chaired by Sandrine Blazy and Marsha Chechik

6.1.2.2. Member of the Conference Program Committees

- CoqPL 2017 (International Workshop on Coq for PL) : Sandrine Blazy
- CPP 2017 (ACM SIGPLAN Conference on Certified Programs and Proofs) : Delphine Demange
- POPL 2017 (Symposium on Principles of Programming Languages) : Delphine Demange (External Program Committee)
- ESOP 2017 (European Symposium on Programming) : David Pichardie
- CC 2017 (International Conference on Compiler Construction) : David Pichardie
- IFL 2016 (International symposium on Implementation and application of Functional Languages) : Sandrine Blazy
- APLAS 2016 (Asian Symposium on Programming Languages and Systems) : Sandrine Blazy
- VSTTE 2016 (Verified Software: Theories, Tools, and Experiments) : Sandrine Blazy, Frédéric Besson
- GPCE 2016 (Generative Programming: Concepts & Experiences) : Sandrine Blazy
- DS@STAF 2016 (Doctoral Symposium) : Sandrine Blazy
- CPP 2016 (Certified Proofs and Programs) : Sandrine Blazy
- HaTT 2016 (International Workshop - Hammers for Type Theories) : Frédéric Besson
- AFADL 2016 (Approches Formelles dans l'Assistance au Développement de Logiciels) : Sandrine Blazy
- iFM 2016 (International Conference on integrated Formal Methods) : Delphine Demange
- FTfJP 2016 (Workshop on Formal Techniques for Java-like Programs) : Delphine Demange
- IFIP SEC 2016 (31st International Conference on ICT Systems Security and Privacy) : Thomas Jensen

6.1.2.3. Reviewer

- POPL 2017 (Symposium on Principles of Programming Languages): Alan Schmitt

- ESOP 2017 (European Symposium on Programming): Alan Schmitt
- VMCAI 2017 (International Conference on Verification, Model Checking, and Abstract Interpretation) : Delphine Demange

6.1.3. Journal

6.1.3.1. Reviewer - Reviewing Activities

- Journal of Software Evolution and Process: Sandrine Blazy
- International Journal of Computer Mathematics: Alan Schmitt
- Science of Computer Programming: Alan Schmitt

6.1.4. Invited Talks

- Journées nationales 2016 GDR Informatique Mathématique : Delphine Demange

6.1.5. Leadership within the Scientific Community

- Thomas Jensen is director of the Department NUMERIC of informatics, mathematics and electrical engineering at University Bretagne Loire.
- Thomas Jensen is leader of the security track of the LABEX Comin Labs.

6.1.6. Scientific Expertise

- Sandrine Blazy: expertise of 1 ANR project.
- Thomas Jensen: expertise of full project proposals for the ANR.

6.1.7. Research Administration

- Sandrine Blazy is member of Section 6 of the national committee for scientific research CoNRS from Sept. 2016.
- Sandrine Blazy is coordinator of the LTP (Languages, Types, Proofs) group of the French GDR GPL.

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

Licence : Sandrine Blazy, Functional programming, 30h, L3, Université Rennes 1, France

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

Licence: Delphine Demange, Functional Programming, 75h, L1, Université de Rennes 1, France

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

Licence : Alan Schmitt, Programmation Fonctionnelle, 72h (2 semestres), L3, Insa Rennes, France

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

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

Master : Sandrine Blazy, Méthodes Formelles pour le développement de logiciels sûrs, 53h, M1, Université Rennes 1, 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 : David Pichardie, Mechanized Semantics, 15h, M2, Université Rennes 1, France

Master : Sandrine Blazy, Mechanized Semantics, 15h, M2, Université Rennes 1, France

Master : Sandrine Blazy, Semantics, 24h, M1, Université Rennes 1, France

Master : David Cachera, Semantics, 24h, M1, Université Rennes 1, France

Master : Sandrine Blazy, Software vulnerabilities, 20h, M2, Université Rennes 1, France

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

Master : Thomas Jensen, Program analysis and Software Security, 36h, M2, Université Rennes 1, France.

6.2.2. Supervision

PhD in progress : Alexandre Dang, Compiler for security, Octobre 2016, Thomas Jensen and Frédéric Besson

PhD in progress : Julien Lepiller, Binary Validation of Software Fault Isolation, Octobre 2016, Thomas Jensen and Frédéric Besson

PhD in progress : Gurvan Cabon, Analyse non locale certifiée en JavaScript grâce à une sémantique annotée, 1st september 2015, Alan Schmitt

PhD in progress : Florent Saudel, Vulnerability discovery, November 2015, Sandrine Blazy, Frédéric Besson and Dimitri Kirchner (Amossys)

PhD in progress : Alix Trieu, Formally verified compilation and static analysis, January 2016, Sandrine Blazy and David Pichardie

PhD in progress: David Bühler, Communication between analyses by deductive verification and abstract interpretation, November 2013, Sandrine Blazy and Boris Yakobowski (CEA)

PhD in progress : Yon Fernandez De Retana, Verified Optimising Compiler for high-level languages, 1st september 2015, David Pichardie and Delphine Demange

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

PhD in progress : Oana Andreescu, Static analysis of functional specifications, 1st September 2013, Thomas Jensen, Stéphane Lescuyer (Prove & Run)

PhD in progress: Pauline Bolignano, Modeling and abstraction of system software, 1st November 2013, Thomas Jensen, Vincent Silés (Prove & Run)

Pierre Wilke, Formally verified compilation of low-level C code, Sandrine Blazy and Frédéric Besson, defended Nov 2016

Martin Bodin, Certified Analyses of JavaScript, Thomas Jensen and Alan Schmitt, defended Nov 2016

6.2.3. Juries

Sandrine Blazy, jury member (reviewer) for the PhD defense of Stefania Dumbrava, December 2016, Paris-Sud University, France

Sandrine Blazy, jury member (reviewer) for the PhD defense of Léon Gondelman, December 2016, Paris-Sud University, France

Sandrine Blazy, jury member (president) for the PhD defense of Thomas Degueule, December 2016, Rennes 1 University, France

Sandrine Blazy, jury member (president) for the PhD defense of Arjun Suresh, May 2016, Rennes 1 University, France

Sandrine Blazy, jury member for the selection of Inria CR (researcher) candidates, March and April 2016, Inria, Saclay, France.

Sandrine Blazy, jury member for the selection of a professeur at University of Perpignan, May 2016, Perpignan, France.

Alan Schmitt, jury member for the selection of Inria CR (researcher) candidates, March and April 2016, Inria, Rennes, France.

Delphine Demange, jury member for the selection of a Maître de Conférences at University Paris Diderot (Paris 7) / IRIF, May 2016, Paris, France.

Alan Schmitt, jury member (reviewer) for the PhD defense of Régis Spadotti, May 2016, Université Toulouse III

Alan Schmitt, jury member (reviewer) for the HDR defense of Nicolas Tabareau, November 2016, Université de Nantes

Thomas Jensen, jury member (reviewer) for the PhD defense of Denis Martinez, February 2016, Université de Montpellier

Thomas Jensen, jury member for the PhD defense of Oliver Schwarz, October 2016, KTH, Stockholm, Sweden

Thomas Jensen, jury member (reviewer) for the PhD defense of Rabah Laouadi, December 2016, Université de Montpellier

David Pichardie, jury member for the PhD defense of Jacques-Henri Jourdan, May 2016, Université de Paris Diderot

6.3. Popularization

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

DEDUCTEAM Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

G. Dowek has co-organized the meeting Universality of Proofs in Dagstuhl.

8.1.1.2. Member of the Organizing Committees

G. Dowek is a member of the steering committee of FSCD.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

F. Blanqui was member of the program committee of the 2016 Coq Workshop.

8.1.2.2. Reviewer

F. Blanqui reviewed papers for IJCAR 2016 and CSL 2016.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

G. Dowek is an editor of TCS-C.

8.1.4. Invited Talks

G. Dowek has been an invited speaker at ISEEP 2016.

G. Dowek has been an invited speaker at Physics and Computation 2016.

8.1.5. Scientific Expertise

G. Dowek has been a member of a commitee dedicated to an update of the high school informatics curriculum.

8.1.6. Research Administration

G. Dowek is the President of the Scientific Board of the Société informatique de France.

G. Dowek is a member of the Scientific Board of la Main à la Pâte.

G. Dowek is a member of the commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene.

G. Dowek is a member of the comité national français d'histoire et de philosophie des sciences et des techniques.

F. Blanqui is co-director of the pole 4 (programming: models, algorithms, languages and architectures) of Paris-Saclay University's doctoral school on computer science.

F. Blanqui is referent of LSV PhD students.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

G. Dowek is attached professor at the École normale supérieure de Paris-Saclay. He has given a course at MPRI. He has given a course to the student preparing the teacher's recruiting exam Agrégation. He is responsible for the second year of master.

F. Blanqui gave a course (15h) on rewriting theory at the MPRI.

8.2.2. Supervision

PhD : Raphaël Cauderlier, Object-Oriented Mechanisms for Interoperability between Proof Systems, CNAM, 10/10/2016, Catherine Dubois

8.2.3. Juries

F. Blanqui was member of the 2016 Inria recruitment committee for young graduate scientists.

F. Blanqui was member of the jury for the best scientific production of the year within Paris-Saclay University's doctoral school on computer science.

GALLIUM Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Michel Mauny is a member of the steering committee of the OCaml workshop.

Didier Rémy was a member of the steering committee of the OCaml workshop until September 2017. He is a member of the steering committee of the ML Family workshop.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Xavier Leroy was a member of the program committees of the Compiler Construction conference (CC 2016), of the conference on Interactive Theorem Proving (ITP 2016), and on the external review committee of the symposium on Principles of Programming Languages (POPL 2017).

François Pottier was a member of the program committees of the conferences Journées Francophones des Langages Applicatifs (JFLA 2017) and Compiler Construction (CC 2017).

10.1.2.2. Reviewer

In 2016, the members of Gallium reviewed at least 30 conference submissions.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Xavier Leroy is area editor (programming languages) for the Journal of the ACM. He is on the editorial board for the Research Highlights column of Communications of the ACM. He is a member of the editorial board of the Journal of Automated Reasoning.

François Pottier is an editor for the Journal of Functional Programming.

10.1.4. Invited Talks

Xavier Leroy was an invited speaker at the ICALP conference (Rome, July 2016).

10.1.5. Research Administration

Xavier Leroy is *délégué scientifique adjoint* of Inria Paris and appointed member of Inria's *Commission d'Évaluation*. He participated in the following Inria hiring and promotion committees: *jury d'admissibilité DR2*, *promotions CR1*, and *promotions DR1*.

Xavier Leroy was a member of the hiring committee for a professor position at Université de Lorraine.

Xavier Leroy was a member of the HCERES evaluation panel for the LORIA laboratory.

François Pottier is a member of the *Commission de Développement Technologique* and (as of January 2016) chairs the *Comité de Suivi Doctoral* of Inria Paris.

Didier Rémy is *Deputy Scientific Director* (ADS) in change of *Algorithmics, Programming, Software and Architecture*.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Xavier Leroy and Didier Rémy, "Functional programming languages", 15+18h, M2 (MPRI), Université Paris Diderot, France.

Master: Luc Maranget, "Semantics, languages and algorithms for multi-core programming", 13.5h, M2 (MPRI), Université Paris Diderot, France.

Master: "Principles of Programming Languages", 32h, M1, ENSTA-ParisTech, France.

Licence: François Pottier, "Programmation avancée" (INF441), 20h, L3, École Polytechnique, France.

Master: François Pottier, "Compilation" (INF564), 20h, M1, École Polytechnique, France.

Licence: Michael Rainey and Umut Acar, "Theory and practice of parallel computing" (part of a longer course entitled 15-210, "Parallel and Sequential Data Structures and Algorithms"), 9h, L3, Carnegie Mellon University, USA.

Michel Mauny has been a Professor at ENSTA-ParisTech from August 1st, 2005 to July 31st, 2016. While at ENSTA-ParisTech, Michel Mauny was in charge of the specialization "Architecture and Security of Information Systems" (MSc. 2nd year).

François Pottier has been a Professeur Chargé de Cours at École Polytechnique from September 1st, 2004 to August 31st, 2016.

Didier Rémy is Inria's delegate in the pedagogical team of the MPRI.

Fabrice Le Fessant has been involved in the second edition of the OCaml MOOC on the FUN platform, in coordination with the OCamlPro team in charge of the development of the exercise platform [33].

10.2.2. Supervision

M2 (Master Pro): Jacques-Pascal Deplaix, Epitech, supervised by François Pottier.

M2 (MPRI): Ambroise Lafont, École Polytechnique, supervised by Xavier Leroy.

PhD: Pierre Halmagrand, "Automated Deduction and Proof Certification for the B Method" [45], Conservatoire National des Arts et Métiers, defended December 10, 2016, supervised by David Delahaye, Damien Doligez and Olivier Hermant.

PhD: Jacques-Henri Jourdan, "Verasco: a formally verified C static analyzer" [11], Université Paris Diderot, defended May 2016, supervised by Xavier Leroy.

PhD: Gabriel Scherer, "Which types have a unique inhabitant?" [12], Université Paris Diderot, defended March 2016, supervised by Didier Rémy.

PhD in progress: Vitalii Aksenov, "Parallel Dynamic Algorithms", Université Paris Diderot, since September 2015, supervised by Umut Acar (co-advised with Anatoly Shalyto, ITMO University of Saint Petersburg, Russia).

PhD in progress: Thomas Blanc (ENSTA-ParisTech & OCamlPro), "Analyses de programmes complets, application à OCaml", Université Paris-Saclay, since February 2014, supervised by Michel Mauny and Pierre Chambart (OCamlPro).

PhD in progress: Pierrick Couderc (ENSTA-ParisTech & OCamlPro), "Typage modulaire du langage intermédiaire du compilateur OCaml," Université Paris-Saclay, since December 2014, supervised by Michel Mauny, Grégoire Henry (OCamlPro) and Fabrice Le Fessant.

PhD in progress: Albin Coquereau (ENSTA-ParisTech), "Amélioration de performances pour le solveur SMT Alt-Ergo: conception d'outils d'analyse, optimisations et structures de données efficaces pour OCaml," Université Paris-Saclay, since October 2015, supervised by Michel Mauny, Sylvain Conchon (LRI, Université Paris-Sud) and Fabrice Le Fessant.

PhD in progress: Armaël Guéneau, “Towards Machine-Checked Time Complexity Analyses”, Université Paris Diderot, since September 2016, supervised by Arthur Charguéraud and François Pottier.

PhD in progress: Thomas Williams, “Putting Ornaments into practice”, Université Paris Diderot, since September 2014, supervised by Didier Rémy.

10.2.3. Juries

François Pottier was a reviewer for the Ph.D. thesis of Benoît Vaugon, Université Paris-Saclay, March 2016. He was a reviewer for the Habilitation of Damien Pous, ENS Lyon, September 2016. He was a member of the jury for the Ph.D. thesis of Léon Gondelman, Université Paris-Saclay, December 2016.

Xavier Leroy was on the Ph.D. committee of Pierre Wilke, Université Rennes 1, November 2016.

Didier Rémy was chair of the Ph.D. committee of Raphaël Cauderlier, Conservatoire National des Arts et Métiers (CNAM), October 2016.

10.3. Popularization

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

MARELLE Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Selection

7.1.1.1. Chair of Conference Program Committees

Yves Bertot is program co-chair, with Viktor Vafeiadis from MPI-SWS in Germany for the ACM conference *Certified Programs and Proofs* (CPP) to be held in Paris in January 2017. Most of the editorial activities took place in 2016.

7.1.1.2. Member of the Conference Program Committees

- Yves Bertot and Laurent Théry were members of the conference program committee for the conference *Interactive Theorem Proving* (ITP) and *User-Interfaces for Theorem Provers* (UITP).
- Cyril Cohen was a member ot the program committee for the 8th Coq workshop.

7.1.1.3. Reviewer

Cyril Cohen was reviewer for the conferences CSL 2016 and ITP 2016. Laurent Théry was a reviewer for the conferences TACAS'17 and CPP'17. Benjamin Grégoire was a reviewer for TACAS. Benjamin Grégoire was a reviewer for PoPL 2017.

7.1.2. Journal

7.1.2.1. Reviewer - Reviewing Activities

Cyril Cohen was a reviewer for *Journal of Automated Reasoning*. Laurent Théry was a reviewer for *Journal of Automated Reasoning* and *Journal of Symbolic Computation*. Yves Bertot was a reviewer for *Journal of Automated Reasoning* and *Computational Geometry: Theory and Applications*.

7.1.3. Invited Talks

Laurent Théry gave an invited talk at MAP'16 (*Mathematics, Algorithms, and Proofs*).

Cyril Cohen gave an invited talk at the ELFIC seminar on the Paris-Saclay campus (Elfic stands for *Éléments finis formellement vérifiés*).

7.1.4. Leadership within the Scientific Community

Yves Bertot and Maxime Dénès have been working on setting up a Consortium of users for the Coq system. The consortium should start in the early days of 2017. Yves Bertot, Enrico Tassi, and Maxime Dénès were invited to the kick-off meeting of the *Expedition in Computing* entitled "the science of deep specification" funded by the NSF foundation, along with three other developers from the pi.r2 project-team, as expert developers of the Coq system. This kick-off meeting took place in June.

7.1.5. Scientific Expertise

- Laurent Théry evaluated projects for the French national agency for research funding (ANR),

7.1.6. Research Administration

- José Grimm is a member of the local committee for Hygiene and Work safety,
- Cyril Cohen served several times as secretary for the local committee of project-team leaders,
- Benjamin Grégoire is a member of the committee on computer tools usage (CUMI) for the Sophia-Antipolis Méditerranée Inria center.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence : Cyril Cohen, mathematics oral exam, 30 hours, Classes préparatoires aux grandes écoles

Master : Laurent Théry gave a course at ENS Lyon (9 hours), a course at École des Mines (3 hours), and a course at University de Marseille (3 hours). Yves Bertot gave a one-week introductory course on Coq at University of Nice (21 hours). Enrico Tassi organized a one-week advanced course on Coq and Mathematical Components for students of ENS Lyon and University of Nice (30 hours). There were two instances of this school, in January and in November, teachers for this course were Enrico Tassi, Yves Bertot, Cyril Cohen, Laurence Rideau, and Laurent Théry.

7.2.2. Supervision

PhD in progress : Boris Djalal, started in October 2015, supervised by Yves Bertot and Cyril Cohen

PhD in progress : Cécile Baritel-Ruet, started in October 2016, supervised by Yves Bertot and Benjamin Grégoire

PhD in progress : Sophie Bernard, started in October 2016, supervised by Yves Bertot and Laurence Rideau

PhD in progress : Damien Rouhling, started in October 2016, supervised by Yves Bertot and Cyril Cohen.

7.2.3. Juries

Yves Bertot was member of the defense committee for the thesis of Jacques-Henri Jourdan.

7.3. Popularization

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

MEXICO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. LIA INFORMEL

The Indo-French Formal Methods Lab is an International Associated Laboratory (LIA) fostering the scientific collaboration between India and France in the domain of formal methods and applications to the verification of complex systems. Our research focuses on theoretical foundations of games, automata, and logics, three important tools in formal methods. We study applications to the verification of safety-critical systems, with an emphasis on quantitative aspects (time, cost, energy, etc.), concurrency, control, and security protocols. The Laboratory was founded in 2012 by a consortium of researchers from the French Centre for Scientific Research (CNRS), Ecole Normale Supérieure de Cachan (ENS Cachan), Université Bordeaux 1, the Institute of Mathematical Sciences Chennai (IMSc), the Chennai Mathematical Institute (CMI), and the Indian Institute of Science Bangalore (IISc). It is directed by Paul Gastin (ENS Cachan, MExICo team) and Madhavan Mukund (CMI). The LIA has been scientifically extremely active and productive since its creation. The LIA has supported numerous scientific exchanges and joint research papers, see here. Among many other activities, the LIA organised another edition of the ACTS workshop.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Thomas Chatain was a member of the program committee of *(ACSD 2016)*.
- Matthias Függer was a member of the PCs of DDECS'16 and ASYNC'16.
- Stefan Haar was a member of the PCs of *13th International Workshop on Discrete Event Systems*WODES 2016, the *16th International Conference on Applications of Concurrency to Systems Design(ACSD 2016)*, *Int. WS on Petri Nets and Software Engineering PNSE 2016*, ATAED Workshop on Analysis of Event Data 2016, and *IEEE Int. Conf. on Emerging Technologies and Factory Automation(ETFA)* 2016.
- Serge Haddad was a member of the PC of the 10th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2016),Tunis, Tunisia.
- Stefan Schwoon was a member of the PC of the 37th International Conference on Applications and Theory of Petri Nets and Concurrency (PN 2016).
- Claudine Picaronny was a PC member for the Eighth International Conference on Advances in System Simulation (SIMUL'16)

9.1.2.2. Reviewer

- Matthias Függer was a reviewer for ICALP, ASYNC, DISC, DDECS, and IPDPS.
- Stefan HAAR was a reviewer for MFCS 2016.
- Stefan Schwoon acted as a reviewer for the following conferences taking place in 2016 : TACAS, ACSD, CONCUR, FSTTCS.

9.1.3. Journal

9.1.3.1. Member of Editorial Boards

- Stefan Haar is an associate editor of the *Journal of Discrete Event Dynamic Systems: Theory and Applications*, and a guest editor (with R. Meyer) of the upcoming special issue on ACSD 2015 in *ACM Transactions on Embedded Computing Systems (TECS)*.

9.1.3.2. Reviewer - Reviewing Activities

- Matthias Függer was a reviewer for the Journal *Energies*.
- Stefan Haar was a reviewer for *LMCS*, *MSCS*, *IEEE Transactions on Automatic Control* and *Journal of Discrete Event Dynamic Systems*.
- Stefan Schwoon acted as a reviewer for the following journals in 2016 : Fundamenta Informaticae, Transactions on Software Engineering.

9.1.4. Invited Talks

- Serge Haddad gave the following invited talks:
  - at the Joint AFSEC/ANR PACS workshop on May 26, 2016, Paris, France, on "Polynomial Interrupt Timed Automata";
  - at the VECOS 2016 conference, Tunis, Tunisia, on October 6, 2016, "Active Diagnosis";
  - at IDC 2016 (10th International Symposium on Intelligent Distributed Computing), October 11, 2016, Paris, France, on "Fault Diagnosis in Probabilistic Systems".
- Benedikt Bollig gave an invited tutorial at Highlights, Brussels, Belgium, 2016, on Automata and Logics for Distributed Systems

9.1.5. Research Administration

- Paul Gastin is one of the directors of the LIA INFORMEL.
- Stefan Haar is the head of the *SCILEX* axis within the *DIGICOSME* Labex. He was the Inria center of Saclay's correspondent for european partnerships until the summer of 2017, when he stepped down from this position to accept the presidency of Inria's COST-GTRI (international relations working group).
- Serge Haddad was a member of the recruitment committee for a professorship at INSA Toulouse.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Serge Haddad and Paul Gastin are professors at ENS Cachan (now ENS Paris-Saclay), Claudine Picaronny, Thomas Chatain and Stefan Schwoon are associate professors of the same university. Serge Haddad is the head of the Computer Science Department, and Stefan Schwoon is in charge of the L3 class. Claudine Picaronny is a co-director of the ENS Paris-Saclay's Mathematics department and a member of the juries of 'l'agrégation interne de Mathématiques' and of the second 'concours de Mathématiques' of ENS Cachan; she is also the coordinator of the mathematics/computer science examination of E3A, parts MP and MC.

Master : Benedikt Bollig, Non-sequential Theory of Distributed Systems, 36, M2, MPRI, ENS Cachan, France.

9.2.2. Supervision

Defended theses:

- PhD ([3])by Salim Perchy , 'Opinions, Lies and Knowledge. An Algebraic Approach to Mobility of Information and Processes', E´cole Polytechnique, defended October 4, supervised by Stefan Haar and Franck Valencia (COMETE team).
- PhD by Simon Theissing [4], 'Supervision for Multimodal Tranport Systems', ENS Cachan, defended December 5, supervised by Stefan Haar.

PhD in progress:

- Tymofii PROKOPENKO, Ecole Polytechnique since Oct 1, 'Privacy', jointly supervised by Catuscia Palamidessi (COMETE team) and Serge Haddad;
- Engel Lefaucheux, ENS Paris-Saclay since 2015, 'controlling information in probabilistic systems', jointly supervised by Nathalie Bertrand (SUMO team) and Serge Haddad

- Yann Duplouy, ENS Paris-Saclay since 2015,'application of formal methods to the development of embedded systems for autonomous vehicles', supervised by Béatrice Bérard and Serge Haddad. Marie Fortin (ENS Paris-Saclay since Oct 1); 'Tree-automata techniques for the analysis of distributed systems', co-supervised by Benedikt Bollig and Paul Gastin.
- Hugues Mandon (ENS Paris-Saclay since Oct 1, Digicosme Grant), Computational Models and Algorithms for the Prediction of Cell Reprogramming Strategies; supervised by Stefan Haar, co-supervision by Loic Paulevé (LRI).
- Robert Najvirt (TU Wien, Austrian FWF SIC project), *realistic delay models with applications in high-speed and low-power circuits*, co-supervised by Matthias Függer and Andreas Steininger.
- Martin Perner (TU Wien, Austrian FWF SIC project), *clock generation on-chip and formalisms suitable to prove correct VLSI circuits*, co-supervised by Matthias Függer and Ulrich Schmid.
- Juergen Maier (TU Wien, Austrian FWF SIC project), *on realistic delay models with applications in high-speed and low-power circuits, with focus on noise and high-order models*, co-supervised by Matthias Függer and with Ulrich Schmid.

9.2.3. Juries

- Benedikt bollig was
  - reviewer and jury member of the PhD thesis Logics on Data Words: Expressivity, Satisfiability, Model Checking by Ahmet Kara (Supervisor: Thomas Schwentick), Universität Dortmund, Germany, 2016, and
  - Reviewer of the PhD thesis Probabilistic Logic, Probabilistic Regular Expressions, and Constraint Temporal Logic by Thomas Weidner (Supervisor: Manfred Droste), Universität Leipzig, Germany, 2016
- Thomas Chatain was a member of the jury for the PhD defense of María Martos-Salgado, Universidad Complutense de Madrid, in January 2016.
- In addition to the juries of the two supervised students, Stefan Haar was the president of the jury for the PhD of Hassan Ibrahim, on 'SAT-based Diagnosability and Predictability Analysis in Centralized and Distributed Discrete Event Systems' at Université Paris-Sud on December 16.
- Serge Haddad was
  - a member of the juries for the PhD of Amira Methni on 'Méthodes de vérification de logiciel système critique", on July 7, 2016, at CNAM,
  - the president of the PhD jury for Hadrien Bride on "Verifying Modal Specifications of Workflow Nets" on October 24, 2016, at Université de Franche-Comté, and
  - a member of the HdR jury for Yann Thierry-Mieg, "From Symbolic Verification To Domain Specific Languages", on December 7, 2016, at Université Paris 6.

9.3. Popularization

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

PARSIFAL Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

D. Miller was on the Steering Committee for the FSCD series of International Conference on Formal Structures for Computation and Deduction.

D. Miller was a member of the jury for selecting the 2016 Ackermann Award (the EACSL award for outstanding doctoral dissertation in the field of Logic in Computer Science).

D. Miller was an ex officio member of the Executive Committee of the ACM Special Interest Group on Logic and Compuation (SIGLOG), from April 2014 to June 2016. He was also a member of the SIGLOG advisory board, starting November 2015.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

D. Miller was on the Program Committee of the following meetings.

FSCD'16: First International Conference on Formal Structures for Computation and Deduction, Porto, Portugal, 22-26 June.

IJCAR 2016: International Joint Conference on Automated Reasoning, Coimbra, Portugal, 27 June - 2 July.

CPP 2016, Fifth International Conference on Certified Programs and Proofs, 18-19 January, Saint Petersburg, Florida.

B. Accattoli was one of the two Program Committee chairs of the 5th International Workshop on Confluence (IWC 2016).

N. Zeilberger served on the program committee for workshops Computational Logic and Applications (CLA 2016) and Off the Beaten Track (OBT 2016).

N. Zeilberger served on external review committee for POPL 2017

L. Straßburger was on the Program Committee for LICS 2016.

9.1.2.2. Reviewer

D. Miller was a reviewer for CONCUR 2016: the International Conference on Concurrency Theory.

B. Accattoli was a reviewer for the international conferences ICTAC 2016, FSCD 2016, LICS 2016 (twice), FOSSACS 2017.

S. Graham-Lengrand was a reviewer for the international conferences FSCD 2016 (twice), LICS 2016 (three times), Concur 2016, VSTTE 2017, HATT 2017, FSTTCS 2017.

L. Straßburger was a reviewer for the international conferences LICS 2016 (8 times), FLOPS 2016.

M. Volpe was a reviewer for the international conferences IJCAR 2016 and CSL 2016.

H. Steele was a reviewer for the internal conference LICS 2016.

9.1.3. Journal

9.1.3.1. Member of the editorial boards

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).

9.1.3.2. Reviewer - Reviewing Activities

S. Graham-Lengrand has been a reviewer for the journals *Fundamenta Informaticae*, *Transactions on Computational Logic*, *Journal of Logic and Computation*, *Logical Methods in Computer Science*, *Journal of Automated Reasoning*.

Danko Ilik was a reviewer for Mathematical Reviews and Zentralblatt MATH.

F. Lamarche was a reviewer for *Mathematical Structures in Computer Science*.

Lutz Straßburger was a reviewer for the journals *Theoretical Computer Science* and *Logical Methods in Computer Science*.

Marco Volpe was a reviewer for the journal *Annals of Mathematics and Artificial Intelligence*.

Beniamino Accattoli was a reviewer for the journals *Theoretical Computer Science* and *Logical Methods in Computer Science*.

9.1.4. Invited Talks

D. Miller was an invited speaker at the following conferences and workshops.

Workshop on linear logic, mathematics and computer science as part of "LL2016-Linear Logic: interaction, proofs and computation", 7-10 November 2016, Lyon. France.

Linearity 2016. Porto, 25 June 2016.

CIPPMI (Current issues in the philosophy of practice of mathematics and informatics) Workshop on Proofs, justifications and certificates. 3-4 June 2016, Toulouse, France.

TYPES 2016: 22nd International Conference on Types for Proofs and Programs. Novi Sad, Serbia, 23-26 May 2016.

D. Miller was an invited speaker at the research seminar titled "Interactions between logic, computer science and linguistics: history and philosophy", Université de Lille 3, 15 June 2016.

D. Miller was an invited speaker at the ACADIA research centre, Ca' Foscari University, Venice, 27 April 2016.

B. Accattoli was invited speaker at WPTE 2016: 3rd International Workshop on Rewriting Techniques for Program Transformations and Evaluation (Porto, 23 June 2016).

S. Graham-Lengrand gave an invited talk at CLAM 2016: 5th Latin American Congress of Mathematicians, thematic session on Logic and Computability (Barranquilla, Colombia, 15th July 2016).

N. Zeilberger was an invited lecturer at OPLSS 2016: Oregon Programming Languages Summer School on Types, Logic, Semantics, and Verification.

9.1.5. Leadership within the Scientific Community

D. Miller was a member of the ACM SIGLOG Advisory Board, the LICS Organizing Board, the CPP Steering Committee, and the ACM SIGLOG Executive Committee Nominating Committee.

S. Graham-Lengrand is the head of the National Workgroup on "Logic, Algebra, and Computation", within the Informatique Mathématique section of CNRS.

9.1.6. Research Administration

L. Straßburger serves on the "commission développement technologique (CDT)" for Inria Saclay–Île-de-France since June 2012

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: D. Miller, "*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*", 12 hours, M2, Master Parisien de Recherche en Informatique, France.

Licence: S. Graham-Lengrand, "*INF412: Fondements de l'Informatique: Logique, Modèles, Calcul*", 32 hours eq. TD, L3, École Polytechnique, France.

Master: S. Graham-Lengrand, "*INF551: Computational Logic*", 45 hours eq. TD, M1, École Polytechnique, France.

Master: S. Graham-Lengrand, "*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*", 6 hours, M2, Master Parisien de Recherche en Informatique, France.

Undergraduate: K. Chaudhuri, R. Blanco, M. Volpe, G. Reis, T. Libal all taught or tutored exercises for first and second year undergrad courses, mostly at École Polytechnique.

9.2.2. Supervision

PhD in progress: Sonia Marin, 1 Nov 2014, supervised by L. Straßburger and D. Miller

PhD in progress: Roberto Blanco, Ulysse Gérard, and Quentin Heath, supervised by D. Miller

PhD in progress: François Thiré (since 1st October 2016), supervised by S. Graham-Lengrand (joint with G. Dowek)

9.2.3. Juries

Miller was a reporter for the PhD juries of Raphaël Cauderlier (CNAM, 10 October 2016) and Gabriel Scherer (Université Paris-Diderot, 30 March 2016).

Graham-Lengrand was a reporter for the PhD juries of Pierre Halmagrand (CNAM, 10 December 2016).

PI.R2 Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Organisation

7.1.1.1. Member of the Organizing Committees

Yann Régis-Gianas is multimedia chair of the organizing committee of POPL 2017 that will be held in Paris in January 2017.

Yves Guiraud, Philippe Malbos and Samuel Mimram have organised the second edition of the Higher-Dimensional Rewriting and Applications (HDRA) workshop of the Formal Structures for Computation and Deduction conference (FSCD), held in Porto in June 2016. They plan to organise the third edition of HDRA, still with FSCD, in September 2017 in Oxford.

Yves Guiraud and Alexis Saurin, with Christine Tasson (IRIF), have organised the annual meeting of the Géocal and LAC working groups of the GDR Informatique Mathématique in Paris, in November 2016.

Yves Guiraud and Samuel Mimram, with Dimitri Ara (Univ. Aix-Marseille) are currently organising the Categories in Homotopy and Rewriting one-week conference, that will be held at the CIRM, in Marseille, in September 2017.

7.1.2. Scientific Events Selection

7.1.2.1. Member of the Conference Program Committees

Matthieu Sozeau was member of the program committees of FSCD'16, ITP'16 and CoqPL'16.

7.1.2.2. Member of the Conference Steering Committees

Hugo Herbelin is a member of the steering committee of the conference *Formal Structures for Computation and Deduction* (FSCD).

Pierre-Louis Curien is member of the steering committee of the international workshop Games for Logic and Programming Languages (GaLop).

Matthieu Sozeau is member of the steering committee of the Dependently Typed Programming international workshop (DTP).

7.1.3. Journal

7.1.3.1. Member of the Editorial Boards

Pierre-Louis Curien is editor in chief of the Cambridge University Press journal Mathematical Structures in Computer Science (since January 2016).

7.1.3.2. Reviewer - Reviewing Activities

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

7.1.4. Invited Talks

Pierre-Louis Curien and Samuel Mimram gave invited talks at the annual meeting of the Géocal and LAC working groups of the GDR Informatique Mathématique (Paris, November).

Pierre-Louis Curien gave an invited talk at the annual meeting of the international ANR project Pace (between Univ. of Bologna, ENS Lyon and Shanghai Jiaotong University) on "Categorified cyclic operads" (Shanghai, November).

Hugo Herbelin gave an invited talk on “Proving with side-effects” at the Days in Logic meeting in Lisbon, Portugal.

Jean-Jacques Lévy gave an invited talk about “Strongly connected components in graphs, Formal proof of Tarjan 1972 algorithm” at the LTP (Langages, Types et Preuves) day, Saclay [38].

Matthieu Sozeau gave invited talks at the DeepSpec kickoff meeting in Princeton, NJ, USA, June 8th 2016, on “Coq 8.6” (together with Maxime Dénès), at the International Conference on Mathematical Software in Berlin, Germany, July 14th 2016, on “Coq for HoTT”, at the Categorical Logic and Univalent Foundations workshop, Leeds, UK, July 28th 2016, on “Forcing Translations in Type Theory”, and at the Coq Workshop in Nancy, France, August 26th 2016, on “Coq 8.6”.

7.1.5. Scientific Expertise

Pierre-Louis Curien has been member of the “Comité de Sélection” for a professor position in discrete mathematics at the University Paul Sabatier in Toulouse.

Yann Régis-Gianas and Hugo Herbelin have been members of the “Comité de Sélection” for an assistant professor position at CNAM in Paris.

Yann Régis-Gianas has been member of the “Comité de Sélection” for an assistant professor position at IRIF in Paris.

Hugo Herbelin has been member of the “Comité de Sélection” for a starting researcher position at Inria Saclay.

7.1.6. Scientific expertise

Pierre-Louis Curien is a member of the Scientific Committee of the CIRM (since June 2013).

7.1.7. Research Administration

Pierre-Louis Curien, Hugo Herbelin and Yves Guiraud are members of the scientific council of the Computer Science deparment of University Paris 7.

Yves Guiraud is the head of the Preuves, Programmes and Systèmes (PPS) team of the IRIF laboratory (since April 2016), and a member of the IRIF council (since January 2016).

7.1.8. Presentation of papers

Étienne Miquey gave a talk on a computational reduction of dependent choice in classical logic to system F at TYPES’16 (Novi Sad, Serbia, May 2016).

Étienne Miquey gave a talk on realizability games for the specification problem during the workshop Realizability in Uruguay 2016 (Piriápolis, Uruguay, July 2016).

Cyrille Chenavier gave a talk at the workshop IWC, Obergurgl, Austria (September 2016).

Cyrille Chenavier, Maxime Lucas and Jovana Obradović gave talks at the workshop Categories, Homotopy and Rewriting (Toulouse, January) and at the workshop HDRA (Porto, June).

Jovana Obradović presented her works on cyclic operads at the Types Conference 2016 (Novi Sad, Serbia, May 2016) and at the Conference Logic and Applications 2016 (Dubrovnik, Croatia, September).

Hugo Herbelin gave a talk on proving Gödel’s completeness theorem with side-effects at the Mathematics for Computation workshop in Niederalteich, Germany, May 2016.

7.1.9. Talks in seminars

Pierre-Louis Curien gave a talk at the Séminaire de Topologie of the University of Angers on the semantics of dependent types (January).

Yves Guiraud gave a talk in the Séminaire de Combinatoire of the University Paris 7 on an introduction to Squier’s theory (November).

Hugo Herbelin gave a talk on a proof-as-program interpretation of the classical axiom of dependent choice at the Séminaire "Logique et Interactions" of the "Logique de la Programmation" team of the "Institut de Mathématiques de Marseille" (University Aix-Marseille, February).

Yann Régis-Gianas gave a talk about control operators in the history of programming at the Séminaire "Code Sources" organized by Baptiste Mélès.

Yann Régis-Gianas gave a talk about the writing style in programming at the conference "Current issues in the philosophy of practice of mathematics and informatics" (University of Toulouse, April).

Thibaut Girka gave a talk about difference languages at the Gallium seminar (Paris, September 2016) and at the TLP group of the GDR GPL (Saclay, November 2016).

Yann Régis-Gianas gave a talk about difference languages at the LIMA laboratory (Nantes, October 2016) and at the Semantic Working Group of IRIF (Paris, December 2016).

Matthieu Sozeau gave a talk about Equations: a function definition toolbox for Coq at Dagstuhl in March 2016.

Cyrille Chenavier gave a talk about confluence algebras at the Algebra working group of the LMPA, Calais, in February 2016.

Jovana Obradović gave a talk about categorified cyclic operads at the Proof Theory Seminar of the Mathematical Institute of the Serbian Academy of Sciences and Arts (Belgrade, December 2016).

7.1.10. Attendance to conferences, workshops, schools,...

Pierre-Louis Curien attended the conferences Types 2016 in Novi Sad (Serbia, May) and Logic and Applications in Dubrovnik (Croatia, September).

Cyrille Chenavier, Pierre-Louis Curien, Yves Guiraud, Maxime Lucas, Philippe Malbos, Samuel Mimram and Jovana Obradović attended the Category, Homotopy and Rewriting workshop in Toulouse (January 2016).

Cyrille Chenavier, Maxime Lucas, Philippe Malbos and Samuel Mimram attended the HDRA workshop in Lisbon (June 2016).

Hugo Herbelin attended the Days in Logic meeting in Lisbon (Portugal, January), the Mathematics for Computation workshop in Niederalteich (Germany, May), the conferences Types 2016 in Novi Sad (Serbia, May), the Coq coding sprint in Sophia-Antipolis (May-June), the DeepSpec kick-off meeting in Princeton (USA, June), the FSCD conference in Porto (Portugal, June), the Coq workshop and ITP 2016 (Nancy, August), as well as the Dagstuhl seminar on universality of proofs (October).

Jean-Jacques Lévy participated to CPP and POPL 2016 conferences, Saint Petersburgh, USA, January 18-22, and the Robin Milner Award reception, the Royal Society, London, November 24 (X. Leroy (research team Gallium) was awarded).

Matthieu Sozeau attended POPL 2016, ICMS 2016, ITP 2016, the Coq coding sprint, the DeepSpec kick-off meeting in Princeton as well as the Dagstuhl seminar on proofs of functional programs (March).

Théo Zimmermann attended the conference CICM 2016 in Białystok (Poland, July). He gave a talk there to present his PhD subject. He also attended the Coq coding sprint.

7.1.11. Groupe de travail Théorie des types et réalisabilité

This is one of the working groups of PPS, jointly organised by Hugo Herbelin and Matthieu Sozeau.

7.1.12. Groupe de travail Catégories supérieures, polygraphes et homotopie

Several members of the team participate actively in this weekly working group of PPS, organised by François Métayer (IRIF) since 2009.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

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: Hugo Herbelin teaches the course on the proof-as-program correspondence for classical logic and beyond at the LMFI.

Master: Pierre Letouzey teaches two short courses to the LMFI Master 2 students : “Models of programming” and ”Introduction to computed-aided formal proofs”. These two courses come in addition to Pierre Letouzey’s regular duty as teacher in the Computer Science department of Paris 7 (including a course on Compilation to M2-Pro students).

Master: Yann Régis-Gianas took part in the MPRI course entitled “Type systems”: he gave a 12-hour course about generalised algebraic data types, higher-order Hoare logic and dependently typed programming.

Master: Matthieu Sozeau taught the MPRI course on Advanced uses of proof assistants (12 hours + a project), together with Assia Mahboubi (Inria SpecFun).

MOOC: In collaboration with Roberto Di Cosmo and Ralf Treinen, Yann Régis-Gianas has created a MOOC about the OCaml programming language. The first edition took place in 2015, the second edition in 2016.

7.2.2. Supervision

Internship: Yves Guiraud has supervised the M2 internship of Amina Bendjaafar.

Internship: Hugo Herbelin has supervised the L3 internship of Meven Bertrand.

Internship: Hugo Herbelin has supervised the pre-doctoral internship of Théo Zimmermann.

Internship: Yann Régis-Gianas has supervised the M1 internship of Paul Laforgue.

Internship: Yann Régis-Gianas has supervised the M1 internship of Sylvain Ribstein.

PhD (completed): Cyrille Chenavier, supervised by Yves Guiraud and Philippe Malbos, successfully defended in December 2016

PhD in progress: Guillaume Claret, Programmation avec effets en Coq, (started in September 2012), supervised by Hugo Herbelin and Yann Régis-Gianas, defense planned in February 2017.

PhD in progress: Amina Doumane, supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien.

PhD in progress: Thibaut Girka, Differential semantics (started in January 2014), supervised by Roberto Di Cosmo and Yann Régis-Gianas.

PhD in progress: Maxime Lucas, supervised by Yves Guiraud and Pierre-Louis Curien.

Phd in progress: Cyprien Mangin, Dependent Pattern-Matching, induction-induction and higher inductive types, September 2015, supervised by Matthieu Sozeau and Bruno Barras.

PhD in progress: Étienne Miquey, Réalisabilité classique et effets de bords, September 2014, supervised by Hugo Herbelin and Alexandre Miquel.

PhD in progress: Jovana Obradović, Cyclic operads: syntactic, algebraic and categorified aspects, supervised by Pierre-Louis Curien.

PhD stopped: Gabriel Lewertowski, On forcing in type theory, supervised by Matthieu Sozeau and Nicolas Tabareau. Gabriel stopped his PhD in september 2016 and is now working at la Pitié Salpêtrière as an engineer.

PhD starting: Gae¨tan Gilbert, Definitional Proof Irrelevance, supervised by Nicolas Tabareau and Matthieu Sozeau.

PhD starting: Théo Zimmermann, supervised by Hugo Herbelin.

7.2.3. Juries

Pierre-Louis Curien was referee for the habilitations of Emmanuel Haucourt (Paris 7, September) and Samuel Mimram (Paris 7, September). He was president of the jury of the thesis of Matteo Acclavio (Univ. de la Méditerranée, December).

Pierre-Louis Curien (president), Yves Guiraud and Philippe Malbos were members of the jury of the thesis of Cyrille Chenavier (Univ. Paris 7, December).

Hugo Herbelin was referee for the habilitation of Nicolas Tabareau (Nantes, November). He was a referee of the jury of the thesis of Jirka Maršík (LORIA, December).

Matthieu Sozeau was a member of the jury of the thesis of Kevin Quirin (EMN Nantes, December).

Yann Régis-Gianas is a member of the jury of the competitive examination for the entrance to the Écoles Normales Supérieures and the École Polytechnique.

7.3. Popularization

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

SUMO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

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).

Thierry Jéron and Nicolas Markey are members of the steering committee of the european summer school MOVEP (Modélisation et Vérification des Systèmes Parallèles). Nicolas Markey was co-chair of the edition that took place in Genova in July 2016.

Thierry Jéron is member of the steering committee of FMF 2017 (Formal Methods Forum) held in Toulouse in January 2017.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Éric Badouel was Chair of conference program committee of CARI 2016.

10.1.2.2. Member of the Conference Program Committees

Éric Badouel was a member of the programme committee of ATAED 2016.

Nathalie Bertrand served on the Program Committees of the international conferences STACS'16, TACAS'16, Concur'16 and QEST'16.

Loïc Hélouët was member of the program committees of ACSD 2016 (Approaches of Concurrency for Systems Design) and SAM 2016 (System Analysis and Modeling).

Thierry Jéron served on the Program Committees of the following international conferences: ICTSS'16, RV'16, SAC-SVT 2017.

10.1.2.3. Reviewer

Nicolas Markey was reviewer for STACS 2017 and AAAI 2017.

Éric Badouel was reviewer for LICS 2016, VeCos 2016, CARI 2016, TACAS 2016, and ATAED 2016.

Loïc Hélouët was reviewer for SAM'2016, ACSD'2016, DNS'2016, STACS'2016, and ICTAC'2016

Thierry Jéron was reviewer for IEEE CASE & ISAM, CONCUR'16.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Éric Badouel is co-Editor-in-Chief of ARIMA Journal (https://arima.episciences.org/).

10.1.3.2. Reviewer - Reviewing Activities

Éric Fabre was reviewer for IEEE TAC, Automatica, JDEDS, CDC, and JONS.

Hervé Marchand was reviewer for JDEDS and Automatica.

Nathalie Bertrand was reviewer for JACM and JCSS.

Nicolas Markey was reviewer for FMSD and TCS.

Éric Badouel was reviewer for Fundamenta Informaticae and Mathematical review-AMS (MathSciNet).

Loïc Hélouët was reviewer for FAOC, TCS, TECS and Fundamenta Informaticae. He also served as reviewer for Mathematical review-AMS (MathSciNet).

Thierry Jéron was reviewer for FAOC and TECS.

10.1.4. Invited Talks

Nathalie Bertrand was invited speaker at MFPS international conference, and gave a lecture at MOVEP summer school.

Éric Badouel was invited speaker at VeCos 2016.

10.1.5. Scientific Expertise

Thierry Jéron served for the expertise of ANR and ASTRID (ANR/DGA) projects.

10.1.6. Research Administration

Éric Fabre is co-director, with Olivier Audouin, of the joint research lab of Nokia Bel Labs and Inria. He is member of the scientific board of the joint lab of Alstom Transport and Inria and member of the Bureau of the Scientific Board of Inria Rennes Bretagne Atlantique.

Hervé Marchand is chairman of the CUMI in Rennes.

Nathalie Bertrand is a nominated member of CNU27 (Conseil National des Universités, section 27).

Éric Badouel is co-director with Moussa Lo (UGB, Saint-Louis du Sénégal) of LIRIMA, the Inria International Lab for Africa. He is scientific officer for the African and Middle-East region at Inria European and International Partnerships Department and member of the executive board of GIS SARIMA.

Loïc Hélouët, Nathalie Bertrand and Ocan Sankur organize the weekly seminar 68NQRT at IRISA (40 talks each year).

Loïc Hélouët was elected representant of rank B researchers in the *Comité de Centre* of Inria Rennes. He is also part of the bureau of the *Comité de Centre*. He leads the P22 projects with Alstom transports and is responsible for Workpackage 2 of the Headwork ANR.

Thierry Jéron is Member Committee Substitute for COST IC1402 ARVI (Runtime Verification beyond Monitoring). He is member of the IFIP Working Group 10.2 on Embedded Systems. He is member of the COS Prospective of Irisa Rennes and member of the *Comité de Centre* of Inria Rennes. Since 2016 he is *référent chercheur* for the Inria Rennes research center.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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 Superieure de Rennes, France.

Nathalie Bertrand

Licence: "Algorithmics", 18h (eq. TD), L3, Univ. Rennes 1, France.

Master: "Prépa. Agreg.", 40h (eq. TD), Ecole Normale Superieure de Rennes, France.

Loïc Hélouët

Licence: JAVA and algorithmics, L2, 40h, INSA de Renne, France.

Licence : practical studies (development of a small project), 8h, INSA de Renne, France.

Master: "Prépa. Agreg.", 8h (eq. TD)+ mock exams, Ecole Normale Superieure de Rennes, France.

10.2.2. Supervision

- PhD in progress: Engel Lefaucheux, *Controlling information in Probabilistic Systems, Sept. 2015, Nathalie Bertrand, Serge Haddad (LSV, Cachan).*
- *PhD in progress: Karim Kecir,* Régulation et robustesse des systèmes ferroviaires urbains, May 2018, Loïc Hélouët and Pierre Dersin (Alstom).
- PhD in progress: The Anh Pham, *Dynamic Formal Verification of High Performance Runtimes and Applications, Nov. 2016, Thierry Jéron, Martin Quinson (Myriads, Inria Rennes).*
- *PhD in progress: Hugo Bazille,* Diagnosability and opacity analysis of large scale systems, Oct. 2016, Blaise Genest, Éric Fabre.
- PhD in progress: Sihem Cherrared, *Fault management in multi-tenant programmable networks, Oct. 2016, Éric Fabre, Gregor Goessler (Inria Grenoble), Sofiane Imadali (Orange Labs).*

10.2.3. Juries

Éric Fabre was reviewer in the PhD defense committee of Yoann Geoffroy, *A general framework for causality analysis based on traces, for composite systems*, Dec. 2016, Univ. Grenoble Alpes. He was also jury member for the Habilitation defense of Blaise Genest, *Taming Concurrency Using Representatives, March 2016, Univ. Rennes 1.*

Hervé Marchand was member of the PhD defences of Hassan Ibrahim, Analyse à base de SAT de la diagnosticabilité et de la prédictabilité des systèmes à événements discrets centralisés et distribués (Université Paris-Sud, Gif-sur-Yvette), December 2016 and of Toussaint Tigori, *Méthodes de génération d'exécutifs temps réel (Ecole centrale de Nantes, Nantes), in November 2016.*

Nicolas Markey was reviewer in the PhD defense committee of Thanh-Tung Tran (LaBRI; supervised by Igor Walukiewicz and Frédéric Herbreteau).

10.3. Popularization

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

TOCCATA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- S. Boldo, vice-president of the 28th "Journées Francophones des Langages Applicatifs" (JFLA 2017)
- J.-C. Filliâtre, organizer of EJCP (École Jeunes Chercheurs en Programmation du GDR GPL) at Lille on June 27–July 1, 2016. 42 participants. http://ejcp2016.univ-lille1.fr/
- A. Paskevich, program chair of the 9th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE 2017), in collaboration with Thomas Wies (NYU).

10.1.1.2. Member of the Organizing Committees

- S. Conchon, local chair for the 44th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2017), held in Paris, France in January 2017.
- G. Melquiond, web chair for the 23rd IEEE Symposium on Computer Arithmetic (Arith 23), held in Silicon Valley, USA in July 2016.
- S. Boldo, member of the organization committee of the Inria Scientific Days in Rennes (June 2016).

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- S. Boldo, PC of the 23rd IEEE Symposium on Computer Arithmetic (ARITH 2016).
- S. Boldo, PC of the 9th International Workshop on Numerical Software Verification (NSV 2016).
- S. Boldo, PC of the 1st Workshop on High-Consequence Control Verification (HCCV 2016).
- S. Boldo, PC of the 27th "Journées Francophones des Langages Applicatifs" (JFLA 2016).
- A. Charguéraud, PC of the International Workshop on Hammers for Type Theories (HaTT 2016).
- A. Charguéraud, PC of the Workshop on ML (ML 2016).
- G. Melquiond, PC of the 3rd International Workshop on Coq for Programming Languages (CoqPL 2017).

10.1.2.2. Reviewer

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

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- G. Melquiond is a member of the editorial board of *Reliable Computing*.
- 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*.

10.1.3.2. Reviewer - Reviewing Activities

The members of the Toccata team have reviewed numerous papers for numerous international journals.

10.1.4. Invited Talks

- S. Boldo gave an invited lecture at Effective Analysis: Foundations, Implementations, Certification in January 2016 at Marseille, France.
- S. Boldo gave a keynote talk in Cambridge at a local workshop about Testing and Verification in Computational Science.
- A. Charguéraud gave an invited talk at the Royal Society specialist meeting "Verified trustworthy software systems", presenting an interactive interpreter for the semantics of JavaScript, in London, on April 7th.
- S. Conchon gave an invited lecture "Model Checking Modulo Theories with Cubicle" at the 2016 edition of the School for Junior Researchers in Programming (École Jeunes Chercheurs en Programmation, EJCP 2016, http://ejcp2016.univ-lille1.fr/) held in Lille, France.
- A. Paskevich gave an invited lecture "Deductive Program Verification using Why3" at the 2016 edition of the School for Junior Researchers in Programming (École Jeunes Chercheurs en Programmation, EJCP 2016, http://ejcp2016.univ-lille1.fr/) held in Lille, France.

10.1.5. Leadership within the Scientific Community

- C. Paulin, scientific leader of Labex DigiCosme http://labex-digicosme.fr (Digital Worlds: distributed data, programs and architectures), until June 2016. It is 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, dean of the Faculty of Sciences of Université Paris-Sud, since July 2016.

10.1.6. Scientific Expertise

- S. Boldo, member of the reviewing board for the ANR (first step in 2016).
- S. Boldo, member of the 2016 committee for the Gilles Kahn PhD award of the French Computer Science Society.
- S. Conchon and A. Paskevich, members of the *"commission consultative de spécialistes de l'université"*, Section 27, University Paris-Sud since December 2014.
- C. Marché, president of the evaluation committee of the joint Digiteo-DigiCosme call for projects https://digicosme.lri.fr/AAPDigiteoDigiCosme2016. The committee selected 10 thesis projects for funding, among 52 submissions. The committee also selected to support 10 scientific events in the Île-de-France region.
- C. Marché, member of the scientific commission of Inria-Saclay, in charge of selecting candidates for PhD grants, Post-doc grants, temporary leaves from universities ("délégations")
- C. Marché, member of the "Bureau du Comité des Projets" of Inria-Saclay, in charge of examining proposals for creation of new Inria project-teams.
- C. Marché, member of a hiring committee for an associate professor position in computer science at CNAM, Paris, France. (sep-oct 2016)

10.1.7. Research Administration

- S. Boldo, member of the CCD, *commission consultative des doctorants*.
- 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.
- 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 100,000 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"*).
- J.-C. Filliâtre is *correcteur au concours d'entrée à l'École Polytechnique et aux ENS* (computer science examiner for the entrance exam at École Polytechnique and Écoles Normales Supérieures) since 2008.
- C. Marché, director of the ProofInUse Joint Laboratory between Inria and AdaCore, http://www.spark-2014.org/proofinuse
- C. Paulin, member 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.
- C. Paulin, chaired the hiring committee for a professor position in computer science at Université Paris-Sud.
- J.-C. Filliâtre, member of the board of GDR GPL, since January 2016.

10.2. Teaching - Supervision - Juries

10.2.1. 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-Diderot, France.

Master: Fondements de l'informatique et ingénierie du logiciel (FIIL) https://www.lri.fr/~conchon/parcours_fiil/: "Software Model Checking" (M2), S. Conchon (9h), "Programmation C++11 avancée" (M2), G. Melquiond (12h), "Vérification déductive de programmes" (M2), A. Paskevich (10.5h), Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): M1101 "Introduction aux systèmes informatiques", A. Paskevich (36h), M3101 "Principes des systèmes d'exploitation", A. Paskevich (58.5h), IUT d'Orsay, Université Paris-Sud, France.

Licence: "Langages de programmation et compilation" (L3), J.-C. Filliâtre (26h), École Normale Supérieure, France.

Licence: "INF411: Les bases de l'algorithmique et de la programmation" (L3), J.-C. Filliâtre (16h), École Polytechnique, France.

Licence: "Programmation fonctionnelle avancée" (L3), S. Conchon (45h), Université Paris-Sud, France.

Licence: "Introduction à la programmation fonctionnelle" (L2), S. Conchon (25h), Université Paris-Sud, France.

10.2.2. Internships

- Raphaël Rieu-Helft (ENS, Paris) is a pre-PhD student doing an internship for 6 months under supervision of C. Marché, G. Melquiond and A. Paskevich. He is working on the design and the formal verification of a library for unbounded integer arithmetic. Why3 is used for formally verifying the functional behaviour of the library operations. Raphaël is also implementing in Why3 a mechanism for extracting code to the C language, in order to obtain a certified code that runs very efficiently.
- Lucas Baudin (ENS, Paris) is a master 1 intern under the supervision of J.-C. Filliâtre between September 2016 and January 2017. He is working on the inference of loop invariants by abstract interpretation in the tool Why3.

- F. Faissole was a master 2 trainee under the supervision of S. Boldo between March and August 2016. He worked on the formal proof of the Lax-Milgram theorem.

10.2.3. Supervision

PhD: L. Gondelmans, "Obtention de programmes corrects par raffinement dans un langage de haut niveau", Université Paris-Saclay & Université Paris-Sud, December 13, 2016, 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: 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.

PhD in progress: M. Roux, "Model Checking de systèmes paramétrés et temporisés", since Sep. 2015, supervised by Sylvain Conchon.

PhD in progress: M. Pereira, "A Verified Graph Library. Tools and techniques for the verification of modular higher-order programs, with extraction", since May 2015, supervised by J.-C. Filliâtre.

PhD in progress: A. Coquereau, "[ErgoFast] Amélioration de performances pour le solveur SMT Alt-Ergo : conception d'outils d'analyse, optimisations et structures de données efficaces pour OCaml", since Sep. 2015, supervised by Sylvain Conchon, Fabrice Le Fessant et Michel Mauny.

PhD in progress: F. Faissole, "Stabilité(s): liens entre l'arithmétique flottante et l'analyse numérique", since Oct 2016, supervised by S. Boldo and A. Chapoutot.

10.2.4. Juries

J.-C. Filliâtre: president of the PhD committee of A. Djoudi, "Analyse statique au niveau binaire", Université Paris Saclay, France, December 2016.

S. Conchon: examiner of the PhD of M. Morterol,"Méthodes avancées de raisonnement en logique propositionnelle : application aux réseaux métaboliques", Université Paris-Saclay, December 2016.

S. Conchon: reviewer of the PhD of A. Blanchard, "Aide à la vérification de programmes concurrents par transformation de code et de spécifications", Université d'Orléans, December 2016.

S. Conchon: reviewer of the HDR of X. Thirioux, "Verifying Embedded Systems", Institut National Polytechnique de Toulouse, September 2016.

S. Conchon : examiner of the PhD of L. Cabaret, "Algorithmes d'étiquetage en composantes connexes efficaces pour architectures hautes performances", September 2016.

10.3. Popularization

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

VERIDIS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Organization of Scientific Events

10.1.1.1. General Chair, Scientific Chair

Jasmin Blanchette and Stephan Merz, with the help of Anne-Lise Charbonnier of Inria Nancy, organized the *7th International Conference on Interactive Theorem Proving* (ITP 2016) and associated workshops in Nancy, on August 22–27, 2016.

10.1.1.2. Member of the Organizing Committees

Jasmin Blanchette co-organized the *Hammers for Type Theories* (HaTT 2016) workshop at IJCAR 2016 in Coimbra, Portugal.

Pascal Fontaine co-organized the *First SC^2 workshop on Satisfiability Checking and Symbolic Computation* with Erika Abraham (RWTH, Aachen).

Pascal Fontaine co-organized the 5th Workshop on Practical Aspects of Automated Reasoning (PAAR) with Stephan Schulz (DHBW Stuttgart) and Josef Urban (Czech Technical University in Prague).

Dominique Méry was a member of the organizing committees of the workshops F-IDE, BWare, Impex, and Formose.

Dominique Méry, together with Yamine Aït-Ameur (Toulouse) and Shin Nakajima (Tokyo), organized a meeting on *Implicit and explicit semantics integration in proof based developments of discrete systems* in November within the series of NII Shonan meetings.

The International Summer School on Verification Techniques, Systems, and Applications (VTSA) has been organized since 2008 in the Greater Region (Nancy, Saarbrücken, Luxembourg, Liège, and Koblenz), and Stephan Merz and Christoph Weidenbach are co-organizers of VTSA. In 2016, VTSA took place at the end of August in Liège, Belgium.

10.1.2. Selection of Scientific Events

10.1.2.1. Chair of Conference Program Committees

Jasmin Blanchette and Stephan Merz chaired the program committee of the *7th International Conference on Interactive Theorem Proving* (ITP 2016).

Stephan Merz co-chaired the program committee of the Third International Workshop on Formal Reasoning in Distributed Algorithms (FRiDA), organized in May as a satellite of NETYS in Marrakech, Morocco.

10.1.2.2. Member of Conference Program Committees

Jasmin Blanchette served on the program committee of the *International Conference on Tests and Proofs* (TAP).

Pascal Fontaine served on the program committee of the workshop SMT.

Stephan Merz served on the program committees of the international conferences ABZ, ICALP, and ICFEM, and of the workshops ARQNL, FMICS-AVoCS, and GRSRD.

Martin Strecker served on the program committees of ICTERI and ICGT.

Thomas Sturm served on the program committees of CASC and of the SC^2 workshop at SYNACS.

Uwe Waldmann served on the program committee of the workshop PAAR, colocated with IJCAR 2016.

Christoph Weidenbach served on the program committee of IJCAR.

10.1.3. Journals

Stephan Merz, together with Jun Pang of the University of Luxembourg, edited two volumes of a special issue on Formal Engineering Methods in the journal *Formal Aspects of Computing*.

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. Together with Deepak Kapur and Stéphane Demri he edited a special issue of JAR containing selected and extended papers of IJCAR 2014.

10.1.4. Invited Talks

Jasmin Blanchette gave invited talks at the Semantic Representation of Mathematical Knowledge Workshop organized by the Wolfram Foundation and the Fields Institute in Toronto, Canada, at the Sino-German Frontiers of Science Symposium (SINOGFOS) organized by the Humboldt Foundation and the Chinese Academy of Science in Shenzhen, China, at the Workshop on Proofs, Justifications, and Certificates in Toulouse, France, at the Universality of Proof seminar at Schloss Dagstuhl in Wadern, Germany, and at the Prague Inter-Reasonning Workshop (PIWo) in Prague, Czech Republic.

Pascal Fontaine gave an invited talk at the AFSEC day of the GdR GPL, and at GT-Verif day of the GdR IM.

Stephan Merz gave invited talks at the TRS meeting and the JAIST-LORIA workshop in Kanazawa, Japan, on *Satisfiability Checking for Modal Logics via SMT Solving* and on *The Design of the TLA$^+$ Proof System*. He also gave an invited talk at the *Cloud Reliability Workshop* in Shenzhen, China, on *A Formal Analysis of Pastry*.

Thomas Sturm gave an invited talk at ACA 2016 titled *Real Problems over the Reals*.

Christoph Weidenbach gave an invited lecture at the SMT Summer School in Lisbon, Portugal.

10.1.5. Leadership within the Scientific Community

Jasmin Blanchette served as editor of the newsletter of the Association for Automated Reasoning (AAR) and as member of the AAR board.

Jasmin Blanchette and Christoph Weidenbach were elected on the CADE (*Conference on Automated Deduction*) Inc. Board of Trustees. Christoph Weidenbach was elected President of CADE Inc. by the CADE Inc. Board of Trustees.

Jasmin Blanchette is an ex officio member of the steering committee of the conference series *Interactive Theorem Proving*.

Pascal Fontaine is an SMT-LIB manager, together with Clark Barrett (Stanford University) and Cesare Tinelli (University of Iowa). He is a member of the FroCoS steering Committee. He has been an elected CADE trustee since October 2014. He serves as member of the Association for Automated Reasoning (AAR) board.

Stephan Merz is a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*. He is also a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS).

Thomas Sturm is a member of the steering committee of the conference series *Mathematical Aspects of Computer and Information Sciences* (MACIS).

Christoph Weidenbach is a member of the steering committee of IJCAR.

10.1.6. Scientific Expertise

Pascal Fontaine was a panel member for the CASC-25 competition of first-order theorem prover.

Stephan Merz served as an expert for the French Agence Nationale de la Recherche (ANR), the Haut Conseil de l'Évaluation de la Recherche et de l'Enseignement Supérieur (HCERES), and for the European Research Council (ERC).

Christoph Weidenbach served as an expert for GIF (German Israel Foundation), the FWF (Austrian Science Fund) and the DFG (German Science Foundation).

10.1.7. Research Administration

Dominique Méry is the head of the Doctoral School IAEM Lorraine for the University of Lorraine.

Stephan Merz is a member of the Scientific Directorate of the International Computer Science Meeting Center in Schloss Dagstuhl. Until August 2016, he was the head of the PhD committee for computer science of the Doctoral School IAEM Lorraine. Since September 2016, he is the delegate for scientific affairs at the Inria Nancy – Grand Est research center. He is also the delegate for the organization of conferences at Inria Nancy and the coordinator of the CPER *Sciences du Numérique* in Lorraine (2015–2020). He was a member of the hiring committee of junior researchers at Inria Nancy in 2016 and a member of the committee for the SIF thesis award (*Prix Gilles Kahn*).

Christoph Weidenbach is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Jasmin Blanchette, Computational Metaphysics (guest lecturer), 4 HETD, Freie Universität Berlin, Germany.

Licence: Marie Duflot-Kremer, Algorithmique et Programmation 1, 80 HETD L1 Mathématiques, Informatiques Sciences pour l'Ingénieur, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Bases de données 1 et 2, 35 HETD, L2 informatique, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Projet personnel et communication, 50 HETD, L2 informatique, Université de Lorraine, France.

Master : Marie Duflot-Kremer, Vérification de systèmes, 30 HETD, M1 Informatique, Université de Lorraine, France.

Master: Marie Duflot-Kremer and Stephan Merz, Vérification algorithmique, 30 HETD, M2 Informatique, Université de Lorraine, France.

Master: Marie Duflot-Kremer and Stephan Merz, Elements of Model Checking, 36 HETD, M2 Informatique and Master Erasmus Mundus DESEM, Université de Lorraine, France.

Master : Marie Duflot-Kremer and Stephan Merz, Conception et architectures distribuées 24 HETD M1 informatique, Université de Lorraine

Licence : Pascal Fontaine, Structure des ordinateurs, 67 HETD, L2 MIASHS, parcours MIAGE, Université de Lorraine, France.

Licence : Pascal Fontaine, Logique des prédicats, 32 HETD, L2 MIASHS, Université de Lorraine, France.

Master : Pascal Fontaine, Réseaux, 50 HETD, M1 MIAGE, Université de Lorraine, France.

Master : Pascal Fontaine, Génie Logiciel, 30 HETD, M1 MIAGE, IGA Rabbat et Université de Lorraine, Maroc.

Master: Dominique Méry, Models and algorithms, 60 HETD, M1, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Formal model engineering, 24 HETD, M2, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Modeling Systems, 30 HETD, M2, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Modeling Systems, 36 HETD, M2 informatique and Master Erasmus Mundus DESEM, Université de Lorraine, France.

Master: Dominique Méry, Event-B modeling, 8 HETD, NUI Maynooth.

Master: Uwe Waldmann, Automated Reasoning I, 90 HETD, Universität des Saarlandes, Germany.

Master: Uwe Waldmann, Automated Reasoning II, 60 HETD, Universität des Saarlandes, Germany. This lecture received the teaching award of the Computer Science Students Association.

10.2.2. Supervision

PhD: Noran Azmy, An Automated Proof of Correctness for Pastry, Saarland University and Université de Lorraine, defended on November 24, 2016.

PhD: Marek Košta, Computational Logic, Universität des Saarlandes. Defended on December 13, 2016.

PhD in progress: Gabor Alági, Efficient Reasoning in Finite Domains, Saarland University. Supervised by 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: Mathias Fleury, Formalization of Logical Calculi, Saarland University. Supervised by Christoph Weidenbach and Jasmin Blanchette, since 09/2015.

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 and Jasmin Blanchette, since 02/2011.

10.2.3. Thesis committees

Dominique Méry served on the committees for the PhD thesis of Pierre Halmagrand (CNAM) and the habilitation thesis of Brahim Hamid (Université Toulouse Jean Jaurès).

Stephan Merz served as a reviewer for the PhD thesis of Yakoub Némouchi (Université Paris Saclay) and as a PhD examiner for the PhD thesis of Alland Blanchard (Université d'Orléans).

10.3. Science outreach

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

- two days at "Fête de la science" in Nancy (Faculté de Sciences et Technologies and ARTEM);
- a course on Scratch for high school professors in charge of teaching optional course ISN (Informatique et Sciences du Numérique);
- her explanations of three new unplugged activities (data bases, model checking and text compression) have been recorded by Inria and will soon be added to the Youtube channel of Interstice intended for promoting and sharing such activities;
- she is in charge of the scientific part of the second module in the Class'Code project, aiming at training teachers and educators for carrying out computer science activities with childrens aged 8 to 14 years;

- she is a member of two groups including university and secondary school teachers, dedicated to the training of math teachers who now teach computer science to students of age 11 to 18. A day of training was given to high school teachers;
- "Journée femmes de Sciences": one day dedicated to the promotion of science towards 14 year-old girls;
- she is a member of the steering committee preparing an itinerant exposition intended for explaining computer science to the public, to be released in December 2016;
- she presented unplugged outreach activities to the staff at Cité des Sciences (Paris);
- she conducted during five months an experiment on the discovery of programming for golden agers using Scratch;
- she took part in "Pépinière 4.0" and 4.1, explaining computer science concepts to teachers.

CARTE Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Nazim Fatès was a co-organiser of ACA'16 (Fourth International Workshop on Asynchronous Cellular Automata and Asynchronous Discrete Models), a workshop which was held during the ACRI 2016 conference, Fez (Morocco), September 8, 2016.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

- Nazim Fatès was member of the Program Committees of ANTS'16 (10th International Conference on Swarm Intelligence), AUTOMATA'16 (22nd International Workshop on Cellular Automata and Discrete Complex Systems) and ACRI'16 (12th International conference on Cellular Automata for Research and Industry).
- Emmanuel Hainry was member of the Program Committee of Developments in Implicit Computational Complexity (DICE) 2016.
- Mathieu Hoyrup was member of the Program Committee of Computability and Complexity in Analysis (CCA) 2016.
- Romain Péchoux was member of the Program Committee of Ressource Aware Computation (RAC) 2016.
- Simon Perdrix was member of the Program Committees of QPL'16 Quantum Physics and Logic, and IQFA'16 7th IQFA's Colloquium.

8.1.2.2. Reviewer

- Emmanuel Hainry reviewed articles for DICE and ICALP.
- Mathieu Hoyrup reviewed articles for ICALP and STACS.
- Emmanuel Jeandel reviewed articles for STACS and MFCS.
- Romain Péchoux reviewed articles for FOSSACS, ISMVL, RAC, LFA and STACS

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

- Nazim Fatès is a member of the editorial board of the *Journal of cellular automata*.
- Emmanuel Jeandel is member of the editorial board of RAIRO-ITA

8.1.3.2. Reviewer - Reviewing Activities

- Nazim Fatès reviewed articles for *Natural Computing*, the *Journal of statistical physics*, *Advanced in Complex systems*, the *Journal of cellular automata*.
- Emmanuel Hainry reviewed an article for Applicable Analysis and Discrete Mathematics.
- Mathieu Hoyrup reviewed articles for Bulletin of Symbolic Logic, Memoirs of the American Mathematical Society, Transactions of the American Mathematical Society.
- Emmanuel Jeandel reviewed articles for Advances in Mathematics, Journal of Discrete Algorithms and Ergodic Theory and Dynamical Systems.
- Romain Péchoux reviewed articles for AMS Mathematical Review, Information & Computation.

- Simon Perdrix reviewed articles for Quantum Information and Computation.

8.1.4. Invited Talks

- Mathieu Hoyrup was invited to give a talk in the special session “Constructive and computable analysis” of the conference Computability in Europe (CiE) in Paris, June 2016.
- Emmanuel Jeandel gave a talk for the national days of GDR-IM.

8.1.5. Leadership within the Scientific Community

- Nazim Fatès is the vice-chair of the IFIP working group 1.05 on Cellular Automata and Discrete Complex Systems.
- Simon Perdrix co-organised the quantum software workshop during the one-day event on quantum Technologies at the french Ministry of Research (July 5, 2016).

8.1.6. Scientific Expertise

- Emmanuel Jeandel reviewed projects for Agence Nationale de la Recherche

8.1.7. Research Administration

Isabelle Gnaedig is:

- vice-leader of the team CARTE,
- member of the scientific mediation committee at Inria Nancy Grand-Est.

Emmanuel Hainry is:

- member of the CNU (Conseil National des Universités), Section 27.
- organizer of the CARTE Seminar.
- examiner for the admission exam of ENS and École Polytechnique.

Mathieu Hoyrup is:

- principal investigator of a PHC Imhotep with Walid Gomaa (Alexandria E-Just University).
- organizer of the Formal Methods Seminar at Loria.

Simon Perdrix:

- is responsible of GT IQ (groupe de travail Informatique quantique) at the CNRS GdR IM (groupe de recherche Informatique Mathématique).
- has been elected member and scientific secretary at CoNRS (Comité National de la Recherche Scientifique) section 6.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence:

- Isabelle Gnaedig
  - To the limits of the computable, 6 hours, Opening course-conference of the collegium "Lorraine INP", Nancy France
- Emmanuel Hainry
  - Systèmes d’exploitation, 30h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Algorithmique, 40h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Web dynamique, 60h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Bases de données, 30h, L1, IUT Nancy Brabois, Université de Lorraine, France

  - Programmation objet, 12h, L2, IUT Nancy Braboi, Université de Lorraine, Frances
  - Complexité, 30h, L2, IUT Nancy Brabois, Université de Lorraine, France
- Mathieu Hoyrup
  - Bases de la Programmation Orientée Objet, 20 HETD, L2, Université de Lorraine, France
  - Interfaces Graphiques, 10 HETD, L2, Université de Lorraine, 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
  - Data Compression, 45h, L2 Informatique
- Romain Péchoux
  - Programmation orientée objet, 61,5h, L3 MIASHS
  - Programmation orientée objet, 53,5h, L2 MIASHS
  - Outils logiques pour l'informatique, 35h, L1 MIASHS
  - Bases de données, 40h, L3 Sciences de la Gestion
  - Algorithmic complexity, 30h, L3 MIAGE, IGA Casablanca, Morocco.

Master:

- Nazim Fatès
  - Systèmes complexes adaptatifs, 15h ETD, M2, UL, France.
  - Agents intelligents et collectifs, 22h ETD, M1, UL, France.
- Isabelle Gnaedig
  - Design of Safe Software, Coordination of the module, M2, Telecom-Nancy (Université de Lorraine), Nancy, France,
  - Rule-based Programming, 20 hours, M2, Telecom-Nancy (Université de Lorraine), Nancy, France.
- Emmanuel Hainry
  - Complexity and Complex Systems, 12h, M2, FST, Université de Lorraine, France
- Emmanuel Jeandel
  - Algorithmics and Complexity, 30h, M1 Informatique
  - Combinatorial Optimization, 36h, M1 Informatique
- Romain Péchoux
  - Mathematics for computer science, 30h, M1 SCA
  - Advanced Java, 52,5h, M1 MIAGE
  - Implicit Complexity, 15h, M2 Informatique
- Simon Perfrix
  - Pépites Algorithmiques, 6h, M1/M2 at Ecole des Mines de Nancy.

8.2.2. Supervision

- Emmanuel Jeandel and Simon Perdrix supervised the Master Thesis of Renaud Vilmart on ZX-calculs, and the Master Thesis of Arinta Auza-Primandini on quantum circuits with memory.

- Emmanuel Jeandel and Simon Perdrix are advisors of Renaud Vilmart, PhD student (UL) since October 2016.
- Romain Péchoux is coadvisor of Pierre Mercuriali, PhD student, Université de Lorraine (50%, advisor: Miguel Couceiro, PR, Université de Lorraine).

8.2.3. Juries

- Mathieu Hoyrup participated in the jury of the PhD of Ludovic Patey, Université Paris Diderot, February 26.
- Emmanuel Jeandel reviewed the PhD thesis of Rodrigo Torres (Universidad de Concepción, Chile) in January, and participated in the PhD defense of Benoît Chappet de Vangel, Université de Lorraine, November 14th.

8.3. Popularization

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

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

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

COMETE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

Note: In this section we include only the activities of the permanent internal members of Comète.

10.1.1. Scientific events organisation

10.1.1.1. 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 Steering Committee of EACSL, the European Association for Computer Science Logics. Since 2015.

The Steering Committee of CONCUR, the International Conference in Concurrency Theory. Since 2016.

The Steering Committee of FORTE, the International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Since 2014.

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.

10.1.2. Scientific events selection

10.1.2.1. Member of conference program committees

Catuscia Palamidessi is/has been a member of the program committees of the following conferences and workshops:

ICTAC 2017. The 14th International Colloquium on Theoretical Aspects of Computing. Hanoi, Vietnam, 23-27 October 2017.

TASE 2017. The 11th International Symposium on Theoretical Aspects of Software Engineering. Nice, France, 13-15 September 2017.

CONCUR 2017. The 28th International Conference on Concurrency Theory. Berlin, Germany, 5-8 September 2017.

CSL 2017. The 26th EACSL Annual Conference on Computer Science Logic. Stockholm, Sweden, 20-25 August 2017.

ICSOFT-PT 2017. The 12th International Conference on Software Paradigm Trends. Lisbon, Portugal, 24-26 July 2017.

ICALP 2017 (Track B). The 44th International Colloquium on Automata, Languages, and Programming. Warsaw, Poland, 10–14 July 2017.
FORTE 2017. The 37th IFIP International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Neuchâtel, Switzerland, 19-22 June 2017.
CSR 2017. The 12th International Computer Science Symposium in Russia. Kazan, Russia, 8–12 June 2017.
ICTAC 2016. The 13th International Colloquium on Theoretical Aspects of Computing. Taipei, Taiwan, 24-31 October 2016.
LOPSTR 2016. The 26th International Symposium on Logic-Based Program Synthesis and Transformation, 6-8 September 2016.
CONCUR 2016. The 27th International Conference on Concurrency Theory. Québec City, Canada, 23-26 August 2016.
TASE 2016. The 10th International Symposium on Theoretical Aspects of Software Engineering. Shanghai, China, 17-19 July 2016.
FCS 2016. The Workshop on Foundations of Computer Security. Lisbon, Portugal, 27 June 2016.
MFPS XXXII. The Thirty-second Conference on the Mathematical Foundations of Programming Semantics. Carnegie Mellon University, Pittsburgh, USA, 23-26 May 2016.

PhDs in Logic VIII. Darmstadt, Germany, 9-11 May 2016.
UEOP 2016. The 1st Workshop on Understanding and Enhancing Online Privacy. San Diego, USA, 21 February 2016.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

ICDE 2017: IEEE International Conference on Data Engineering
CSF 2017: 30th IEEE Computer Security Foundations Symposium
POST 2017: 6th International Conference on Principles of Security and Trust
BIGQP 2017: International Workshop on Big Geo Data Quality and Privacy
PETS 2016: The 16th Privacy Enhancing Technologies Symposium
WWW 2016: 25th World Wide Web conference
APVP 2016: 7ème 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 2016. The 18th International Symposium on Principles and Practice of Declarative Programming (PPDP 2016).
ICTAC 2016. The 13th International Colloquium on Theoretical Aspects of Computing (ICTAC 2016).
ICLP DC 2016. 12th ICLP Doctoral Consortium.

10.1.2.2. Reviewer

The members of the team reviewed several papers for international conferences and workshops.

10.1.3. Journals

10.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press.
Member of the Editorial Board of Acta Informatica, published by Springer.
Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, published by 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.

10.1.3.2. Reviewer

The members of the team reviewed several papers for international journals.

10.1.4. Other Editorial Activities

Frank D. Valencia has been:

Co-editor of the special issue on Mathematical Structures in Computer Science dedicated to the best papers from the 12th International Colloquium on Theoretical Aspects of Computing.

10.1.5. Other Activities

10.1.5.1. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

DISCOTEC 2016 (Keynote speaker). The 11th International Federated Conference on Distributed Computing Techniques. Crete, Greece, 6-9 June 2016.

Journée sur la Securité, la Sureté et la Confidentialité. Organized by Paris VII, Paris XIII and Systematic. Paris, France, 10 May 2016.

10.1.5.2. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the Alonzo Church Award Committee. Since 2015. This award is for an outstanding contribution to Logic and Computation within the past 25 years.

President of the selection committee for the EATCS Best Paper Award at the ETAPS conferences. Since 2006.

10.1.5.3. Service

Catuscia Palamidessi has served as:

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.

Member of the comité de selection for a position for Maitre de Conferences at l'Université de Paris VII (Paris Diderot). Spring 2016.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). May 2016 - .

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

PhD : Catuscia Palamidessi has been teaching a course for PhD students, on Protection of sensitive information, at the University of Venice, Italy. April 2016. Total 30 hours.

Master : Frank D. Valencia has been teaching the undergraduate course "Computability", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2016.

Master : Frank D. Valencia has been teaching the masters course "Foundations of Computer Science", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. Jan 27 - Jun 1, 2016.

Master: Konstantinos Chatzikokolakis and Catuscia Palamidessi have been teaching a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. 2016-17. Total: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

10.2.2. Supervision

PhD in progress (2016-) Tymofii Prokopenko. Ecole Polytechnique and ENS Cachan. Grant Digiteo-Digicosme. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Serge Haddad.

PhD in progress (2015-) Joris Lamare. Ecole Polytechnique. Grant MSR Center. 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 completed (2013-16) Salim Percy. Ecole Polytechnique. Grant Digiteo-Digicosme. Co-supervised by Frank D. Valencia and Stefan Haar.

10.2.3. Juries

Catuscia Palamidessi has been reviewer and member of the board at the PhD defense for the thesis of the following PhD student:

Huu-Hiep Nguyen, PhD student supervised by Abdessamad Imine, University of Lorraine, France. November 2016. Title of the thesis: Social Graph Anonymization.

10.2.4. Other didactical duties

Catuscia Palamidessi is:

External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.

Member of the Committee d'Encadrement de Thèse of Jun Wang (PhD student supervised by Qiang Tang and Peter Ryan), University of Luxembourg. Since December 2014.

Member of the advising committee for the PhD of Andrea Margheri (PhD student supervised by Rosario Pugliese), University of Florence, Italy. 2014-16.

Konstantinos Chatzikokolakis and Catuscia Palamidessi have designed, and coordinate, a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. 2016-17.

DICE Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

- Ste´phane Frénot, French Tech, représentant de la COMUE de Lyon
- Ste´phane Grumbach, ANR, Comite´ de Pilotage Scientifique du De´fi 8 « Socie´te´s innovantes »
- Ste´phane Grumbach, scientific committee Global Forum
- Ste´phane Grumbach, scientific committee Colle`ge des Bernardins, Journalisme et bien commun a` l'heure des algorithmes

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Stéphane Grumbach has been chair of the following conferences:

- From data on ecosystems to ecosystems of data, Seminar in cooperation between ENS and EPFL, Lausanne, 21 October 2016
- Seminar Intermediation and Smartness, Anthropocene Curriculum, The Technosphere Issue, Haus der Kulturen der Welt, Berlin, 15-23 April 2016

9.1.3. Invited Talks

Stéphane Grumbach has given the following talks:

- Panel The Transatlantic Data War, obama2016: L'héritage Obama. Tensions et reconfigurations après la présidentielle, Paris, 12-14 déc. 2016
- Panel L'impact des algorithmes sur les media et la culture, Entretiens Jacques Cartier, Lyon 21 novembre 2016
- The Datasphere, in control of ecosystems, The 136th RIHN seminar, Research Institute for Humanity and Nature, Kyoto, 18 November 2016
- Digital Platforms, Europe Asia, Diverging Spaces?, The Relevance of Area Studies for the Sciences and Public Policy, DIJ, Tokyo, 14-15 November 2016
- Platforms vs Administrations, The mutation of data driven government, , ECNU, Shanghai, 9 November 2016
- Panel The Data Revolution, Global Forum, Digitalization: the global transformation, Eindhoven, 19-20 September 2016
- Innovation, pouvoir et territoires, Summer School Cespec 2016, (IX Edizione) Futuri. Immaginare il mondo di domani, Cuneo-Savigliano-Alba-Mondovì, 13-17 settembre 2016
- Révolutions dans la culture et la transmission des savoirs à l'heure du numérique, TUBA'X-PERTS, Lyon, 9 juin 2016
- Conférence "Grand Témoins" : le BIG DATA, Grand rendez-vous de la Métropole, Lyon, 23 mars 2016 video
- Géopolitique du numérique : enjeux des plateformes globales pour la région, LeLabIdF, ThinkLab de la Région Île-de-France, Paris, 17 mars 2016
- Intelligence artificielle, le pouvoir aux machines ? Collège des Bernardins, Paris, 11 février 2016

9.1.4. Research Administration

Ste´phane Grumbach is director of IXXI, the complex Systems Institute.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Stéphane Grumbach, Guerre, climat et enjeux de l'Anthropocène, 2h, M1, ENS de Lyon, France

Master : Stéphane Grumbach, La révolution numérique et les difficultés d'ajustement des administrations françaises, 2h, M1, ENTPE, France

Master : Stéphane Grumbach, Réseaux sociaux et Nouveaux Outils de Communication, 2h, M1, INSA Lyon, France

Master : Damien Reimert, - Bitcoin, 24h, M1, INSA de Lyon, France

Master : Damien Reimert, Javascript, 43h, M1, Télécom St-Étienne, France

Licence : Damien Reimert, Développement Mobile, 39h, L3, Télécom St-Étienne, France

Licence : Aurélien Faravelon, HTML5 CSS3 Javascript, 24h, L3, IUT 2 Grenoble, France

Master : Aurélien Faravelon, Economie de l'intermediation, 2h, M2, Ecole centrale de Lyon, France

Licence : Robert Riemann, INSA, Algorithmique et programmation 1, 27HETD, L1, INSA Lyon, France

9.2.2. Supervision

PhD : Etienne Brody, DataFlow compilation from JavaScript, INSA Lyon, 21 Juin, Stéphane Frénot

PhD in progress : Robert Riemann, systemes de vote decentralise´s, sept 2014, Ste´phane Grumbach

9.3. Popularization

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

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

PESTO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting.[0] 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 formulated new recommendations, submitted to the CNIL. They 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 2017.

Moreover, Véronique Cortier was auditioned by the AFE (Assemblée des Francais de l'étranger) on the security of electronic voting. She has also presented the Belenios protocol to the MENESR (Ministère de l'Éducation National, de l'Enseignement Supérieur et de la Recherche) and to the Open Government Summit at the Sénat. Steve Kremer gave a talk on e-voting at the "Colloque Sécurité Informatique : mythes et réalité" organised by CNRS.

10.1.1. Scientific Events Selection

10.1.1.1. General Chair, Scientific Chair

- Véronique Cortier: HotSpot 2016, 4th Workshop on Hot Issues in Security Principles and Trust. Affiliated with ETAPS 2016.
- Steve Kremer: GRSRD 2016, Grande Region Security and Reliability Day, Nancy, March 2016 (co-chair with J. Pang, U. Luxembourg).

10.1.1.2. Program Committee Chair

- Véronique Cortier: HotSpot 2016, 4th Workshop on Hot Issues in Security Principles and Trust. Affiliated with ETAPS 2016.
- Michaël Rusinowitch: ACM International Workshop on Security And Privacy Analytics, New Orleans, LA, USA, March 11, 2016. (co-chair with Rakesh Verma, U. Houston).

10.1.1.3. Program Committee Member

- Véronique Cortier: LICS 2017, CCS 2016, Concur 2016, E-VoteID 2016, MFCS 2016, EuroS&P 2016.
- Steve Kremer : Voting 2017, Euro S&P 2017, FSTTCS 2016, ESORICS 2016, CSF 2016, Voting 2016, AsiaCCS 2016, ACISP 2016.
- Christophe Ringeissen: FroCoS 2017, UNIF 2017, WRLA 2016, UNIF 2016, IJCAR 2016.
- Michaël Rusinowitch: POST 2016, CRISIS 2016, STM 2016.
- Vincent Cheval: TMPA 2017

10.1.2. Journal

10.1.2.1. Editorial Board Member

- Véronique Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Information and System Security (TISSEC), Foundations and Trends (FnT) in Security and Privacy.

10.1.2.2. Scientific Committee Member

- Laurent Vigneron: Technique et Sciences Informatiques, Lavoisier.

10.1.3. Invited Talks

- Steve Kremer: 29th IEEE Computer Security Foundations Symposium (CSF'16).

10.1.4. Research Administration

Inria evaluation committee (Steve Kremer)

[0] https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023174487

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (Steve Kremer)

Jury Senior Research Position (Steve Kremer)

Jury Junior Research Position Inria Nancy-Grand Est (Véronique Cortier, president of the committee)

Jury Professor at Université de Lorraine (Véronique Cortier)

Jury Assistant Professor at Université de Lorraine (Michaël Rusinowitch)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

  Vincent Cheval, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 69 hours (ETD), TELECOM Nancy.

  Jannik Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 146 hours (ETD), TELECOM Nancy.

- Master:

  Véronique Cortier, Security of flows, 20 hours, M2 Computer Science, Telecom Nancy and Mines Nancy, France.

  Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, Lorraine University, France.

  Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.

  Christophe Ringeissen, Decision Procedures for Software Verification, 18 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.

  Laurent Vigneron, Security of information systems, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Lorraine University, France.

10.2.2. Supervision

- HDR defended in 2016:

  Abdessamad Imine, Data sharing in collaborative systems, defended on December 9.

- PhD defended in 2016:

  Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune
  Huu Hiep Nguyen, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch

- PhD discontinued in 2016:

  Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, discontinued in June 2016, Véronique Cortier

- PhD in progress:

  Younes Abid, Privacy control for social networks, started in March 2015. Abdessamad Imine, Michaël Rusinowitch and Orpailleur co-advising.

  Antoine Dallon, Decision procedures for equivalence properties, started in November 2015, Véronique Cortier and Stéphanie Delaune

Alicia Filipiak, Design and validation of security services for mobile platforms: smartphones and tablets, started in March 2015, Véronique Cortier

Joseph Lallemand, Type systems for equivalence properties, started in September 2016, Véronique Cortier

Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Stéphanie Delaune and Steve Kremer

10.2.3. Juries

Reviewer for Yang Zhang PhD, Luxembourg (Michaël Rusinowitch)

Examiner for Stefania Dumbrova, Paris-Sud (Michaël Rusinowitch)

Examiner for Jiri Marsik, LORIA (Laurent Vigneron)

Examiner for Robin David, CEA (Steve Kremer)

10.3. Popularization

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

PRIVATICS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Daniel Le Metayer: CPDP 2016 (panel chairman), Privacy protection, new technical and legal instruments (Colloque Inria CAPPRIS).

Cédric Lauradoux: Nombre et cryptographie, maison pour la science Alpes Dauphiné

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Cédric Lauradoux: RESSI 2016 and ATC 2016.

Daniel Le Metayer: Infer 2016, STM 2016, Annual Privacy Forum 2016, IWPE 2016, CPDP 2016 and WETICE-FISA.

Marine Minier: MyCrypt 2016 and RESSI 2016.

Vincent Roca: GreHack 2016, SPACOMM 2016 and VTC2016-Spring.

Mathieu Cunche: APVP 2016, HotPlanet 2016, ICISSP 2017 and IEEE TrustCom 2016.

Claude Casteluccia: Wisec 2016, DTL 2016, AFP 2016, UEOP'16 and DAT'2016.

9.1.3. Invited Talks

Daniel Le Metayer: IFIP SEC 2016 and France Stratégie, Algorithms: transparency and responsibility panel.

Claude Casteluccia: LIG Keynote.

9.1.4. Leadership within the Scientific Community

Vincent Roca: co-chair of the research group NWCRG (Network Coding Research Group) of IRTF (Internet Research Task Force)

Daniel Le Metayer: member of the scientific committee of the CNIL-Inria Privacy Award

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Undergraduate course : Vincent Roca, *On Wireless Communications*, 12h, L1, Polytech' Grenoble, France.

Undergraduate course : Vincent Roca, *On Network Communications*, 44h, 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.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.

Undergraduate course : Mathieu Cunche, *Advanced Topics in Security*, 20h, L3, ENSIMAG, France.

Undergraduate course : Mathieu Cunche, *Security & Privacy*, 21h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Security & Privacy*, 17h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Privacy*, 12h, L3, INSA-Lyon, France.

Master : Cédric Lauradoux, *Introduction to Cryptology*, 30h, M1, University of Grenoble Alpes, France.

Master : Cédric Lauradoux, *Internet Security*, M2, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 20h, M2, Ensimag/University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.

Master : Claude Castelluccia, *Security & Privacy*, 18h, Master MOSIG, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Privacy*, 4h, M2, College de droit University of Grenoble Alpes, France.

Master : Marine Minier, *Security for wireless networks*, 20h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Master : Daniel Le Métayer, *Privacy*, 6h, M2 MASH, Université Paris Dauphine, France.

9.2.2. Supervision

PhD defended : Jagdish Achara, *Unveiling and Controlling Online Tracking*, Claude Castelluccia and Vincent Roca.

PhD defended : Amrit Kumar, *Security and Privacy of Hash-Based Software Applications* , Cedric Lauradoux.

PhD in progress : Victor Morel, *IoT privacy* , September 2016, Daniel Le Métayer.

PhD in progress : Jessye Dos Santos, *Wireless physical tracking*, October 2013, Cédric Lauradoux and Claude Castelluccia.

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): Alessandro Tedesco, *The rise of Internet of things made possible the large-scale collection of personal data and metadata*, Claude Castelluccia

Intern (M2): Jose-Paul Domingez, *The geopolitics of Internet protocols*, Claude Castelluccia

Intern (M2): Zoltan Kovac, *MyRealOnlineChoices*, Claude Castelluccia

Intern (M1): Margaux Canet Sola, *decompression bombs*, Cédric Lauradoux

Intern (M1): Julie Catania, Fuzzing the `zlib`, Cédric Lauradoux

Intern (M1): Aurelien Monnet Paquet, *Anti-virus DOS attacks*, Amrit Kumar

Intern (M1): Mary-Andrea Rakotomanga, *Compression quines*, Cédric Lauradoux

9.2.3. Juries

PhD: Yagdish Achara, *Unveiling and Controlling Online Tracking*, 18/10/2016, Claude Castelluccia and Vincent Roca.

PhD: Amrit Kumar, *Security and Privacy of Hash-Based Software Applications*, Université de Grenoble, Nantes, 18/10/2016, Cédric Lauradoux.

PhD : Tarek Sayah, *Exposition seélective et probleème de fuite d'inférence dans le Linked Data*, Université Claude Bernard Lyon 1, 8/9/2016, Vincent Roca.

PhD : Karina Sokolova Perez, *Bridging the Gap between Privacy by Design and Mobile Systems by Patterns*, UTT Troyes, 27/04/2016, Daniel Le Métayer.

PhD: Tania Richmond, *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs*, Université de Saint-Etienne, 24/10/2016, Marine Minier.

PhD: Nora El Amrani, *Codes MDS additifs pour la cryptographie*, Université de Limoges, 24/02/2016, Marine Minier.

9.3. Popularization

9.3.1. Interview

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

9.3.2. Articles

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

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

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

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

9.3.3. Conferences

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

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

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

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

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

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

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

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

PROSECCO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Prosecco is organizing the 2nd IEEE European Symposium on Security and Privacy in Paris, | 26-28 April 2017. Catalin Hritcu is General Chair, Bruno Blanchet is Finance Chair, and Karthikeyan Bhargavan is Local arrangements Chair.
- Catalin Hritcu organized two Secure Compilation Meetings (SCM) at Inria Paris in (13 invited participants, 17–19 August 2016) and POPL (15 January 2017)

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Catalin Hritcu is PC member at POPL 2017
- Catalin Hritcu is PC member at POST 2017
- Catalin Hritcu was PC member at CSF 2016
- Catalin Hritcu was PC member at POST 2016
- Catalin Hritcu was PC member at ITP 2016
- Catalin Hritcu was PC member at cPP 2016
- Harry Halpin is PC member for ACM WWW 2017
- Harry Halpin was PC member for W3C Blockchains and the Web
- Karthikeyan Bhargavan is ERC member at POPL 2017
- Karthikeyan Bhargavan is PC member at IEEE S&P 2017
- Karthikeyan Bhargavan was PC member at IEEE S&P 2016
- Karthikeyan Bhargavan was PC member at ACM CCS 2016
- Karthikeyan Bhargavan was PC member at IEEE CSF 2016
- Karthikeyan Bhargavan was PC member at ACM PLAS 2016

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Associate Editor

– of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: Bruno Blanchet

9.1.4. Invited Talks

- Karthikeyan Bhargavan gave an invited talk at EUROCRYPT 2016
- Karthikeyan Bhargavan gave an invited talk at the OAuth Workshop 2016
- Karthikeyan Bhargavan gave an invited talk at SSTIC 2016

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master: Bruno Blanchet, Formal Methods, 9h equivalent TD, master M2 MIC, université Paris VII, France
- Master: Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 31.5h equivalent TD, master M2 MPRI, université Paris VII, France
- Master: Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 31.5h equivalent TD, master M2 MPRI, université Paris VII, France
- Master: Karthikeyan Bhargavan, Protocol Safety and Security, master ACN Telecom ParisTech et Ecole Polytechnique
- Undergraduate: Karthikeyan Bhargavan, INF421 and INF431: Programmation, Ecole Polytechnique
- Doctorat: Karthikeyan Bhargavan: Protecting TLS from legacy cryptography, l'École de printemps en codage et cryptographie, May 2016
- Master: Catalin Hritcu, Cryptographic protocols: formal and computational proofs, 31.5h equivalent TD, master M2 MPRI, université Paris VII, France
- Doctorat: Catalin Hritcu: F* course at Computer Aided Analysis of Cryptographic Protocols summer school, Bucharest, September 2016

9.2.2. Supervision

- PhD completed: Antoine Delignat-Lavaud
  On the Security of Authentication Protocols for the Web
  defended March 2016, supervised by Karthikeyan Bhargavan
- PhD in progress: Evmorfia-Iro Bartzia
  Machine-checked program verification for concrete cryptography,
  defence on February 15, 2017, supervised by Karthikeyan Bhargavan and Pierre-Yves Strub
- PhD in progress: Jean Karim Zinzindohoué
  Analyzing cryptographic protocols and their implementations,
  started September 2014, supervised by Karthikeyan Bhargavan
- PhD in progress: Nadim Kobeissi
  Analyzing cryptographic web applications,
  started February 2015, supervised by Karthikeyan Bhargavan
- PhD incomplete: Yannis Juglaret
  Micro-policies and Secure Compilation,
  started September 2015, interrupted September 2016, supervised by Catalin Hritcu

9.2.3. Juries

- Karthikeyan Bhargavan served on the PhD jury of Olivier Levillain
- Harry Halpin served on the PhD jury of Nikita Mazurov

9.3. Popularization

9.3.1. Seminars

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

TAMIS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Axel Legay has been the general chair for the 11th International Conference on Risks and Security of Internet and Systems

10.1.1.2. Member of Organizing Committees

- Axel Legay has been organizing the ICT-Energy Science Conference 2016.

10.1.2. Scientific Events Selection

10.1.2.1. Member of Conference Steering Committees

- Olivier Zendra is a founder and a member of the Steering Committee of ICOOOLPS (International Workshop on Implementation, Compilation, Optimization of OO Languages, Programs and Systems)

10.1.2.2. Chair of Conference Program Committees

- Axel Legay has been the chair for the 14'International Symposium on Automated Technology for Verification and Analysis

10.1.2.3. Member of Conference Program Committees

- Axel Legay has been PC member for ASE, MEMOCODE, FASE, RV, SPLC, FORMATS, FORMALIZE, SETTA,
- Jean-Louis Lanet has been PC member of Cardis 2016, 15th Smart Card Research and Advanced Application Conference, Crisis 2016 The Eleventh International Conference on Risks and Security of Internet and Systems CRiSIS 2016, GraMSec'16, The Third International Workshop on Graphical Models for Security, June 27th Lisbon, Portugal Ressi 2016, Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, Toulouse, France, Afadl2016, 15èmes Journées Francophones Internationales sur les Approches Formelles dans l'Assistance au Développement de Logiciels.
- Olivier Zendra has been PC member of PEC 2016 (International Conference on Pervasive and Embedded Computing)

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Axel Legay is a funder and member of the editorial board of "Foundations for Mastering Changes" journal.

10.1.3.2. Reviewer - Reviewing Activities

- Axel Legay has been reviewer for TCS, TSE, Information and Computation.

10.1.4. Invited Talks

- Axel Legay has been an invited speaker for the 10th International Workshop on Reachability Problems.
- Axel Legay has been an invited speaker for the ICT-Energy Science Conference 2016.
- The Wheel of Fault Injection, J.-L Lanet, Workshop Sertif, Grenoble, October 2016.

- Christian Grothoff. “Enabling Secure Web Payments with GNU Taler”. Keynote at SPACE 2016 (December).
- Christian Grothoff. “Anonymous Payment Systems” at MAPPING Second General Assembly, Prague, 2016.
- Christian Grothoff. “Netzwerksicherheit: Probleme und Lösungsansätze” at NPO Kongress, Wien, 2016.
- Christian Grothoff. “The GNU Name System: A Public Key Infrastructure for Social Movements in the Age of Universal Surveillance” at Johns Hopkins University, Baltimore, USA, 2016.
- Christian Grothoff. “GNU Taler” at the Free Software Foundation Fellowship Meeting, Düsseldorf, 2016.
- Christian Grothoff. “The GNU Name System: A clean-slate solution to the DNS security and privacy nightmare” at Journée du Conseil scientifique de l’Afnic, Paris, 2016.
- Christian Grothoff. “GNU Taler: A privacy-preserving online payment system for libre society” at CubaConf, Havana, 2016.
- Jeffrey Burdges. “GNU Taler” at the Internet Freedom Festival, 2016.
- Jeffrey Burdges. Preliminary report “Xolotl A compact mixnet format with stronger forward secrecy and hybrid anonymity” at the GNU Hacker Meeting, 2016.
- Florian Dold presented “GNU Taler – Privacy preserving payments for the web” at the GNU Hacker Meeting, 2016.
- Jeffrey Burdges. Panel on “Privacy-preserving decentralization: what challenges are lying ahead?” at the ECRYPT 2016 Workshop on Strategic Research Challenges for Privacy Technologies.
- Christian Grothoff. Panel on "Innovation, Complexity, Risk and Trust" at MAPPING Second General Assembly, Prague, 2016.

10.1.5. Scientific Expertise

- Axel Legay is an expert for the Wallonie Government.
- Axel Legay is a member of Inria’s evaluation committee. He participated to the CR2 and CR1 juries for Lille Center.
- Axel Legay has been in the jury for the chair on cyber security at CentralSupelec.
- Jeffrey Burdges, Christian Grothoff, and Florian Dold have been involved in the W3C Payments Working Group, primarily contributing security and privacy comments on their evolving standard.
- Olivier Zendra is a CIR expert for the MENESR.
- Olivier Zendra is a member of Inria’s evaluation committee. He participated to the CR2 jury for Grenoble Center, to the national CR1 promotion jury, and to the workgroup on the creation of the PACAP team of Inria Rennes.
- Olivier Zendra is a member of the editorial board and co-author of the “HiPEAC Vision” [69]

10.1.6. Research Administration

- Axel Legay is a member of Inria’s evaluation committee.
- Axel Legay is the Representative for non-permanent staff committees (in charge of postdocs).
- Olivier Zendra is a member of Inria’s evaluation committee.
- Olivier Zendra was a member of Inria’s Parity and Equal Opportunities committee.
- Olivier Zendra is a member of Inria’s worksgroup on Inria’s social barometer.
- Olivier Zendra was a member of Inria’s CNHSCT.
- Olivier Zendra was Head of Inria Nancy’s IES Committee (formerly IST).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Master : Axel Legay, Introduction au Model Checking, 36, M2, Université de Bretagne Sud, France
- Master : Axel Legay, Introduction à l'analyse de risques, M2, Université de Bretagne Sud, France

10.2.2. Supervision

- PhD : Aymerick Savary, De la génération de suites de test à partir de modèles formels, University of Sherbrook and University of Limoges, 30th June 2016, Marc Frappier, Jean-Louis Lanet
- PhD : Tiana Razafindralambo, Attaques combinées sur appareil mobiles, University of Limoges, November 2016, Christophe Clavier, Jean-Louis Lanet
- PhD : Neal Walfield, Location prediction for context-aware applications, Johns Hopkins, 4th October 2016, Christian Grothoff
- PhD in progress : Kevin Bukasa, Démarrage sécurisé, 2015, Jean-Louis Lanet and Axel Legay
- PhD in progress : Mounir Chadli (Rennes 1), On Scheduling and SMC, December 2014, Axel Legay and Saddek Bensalem.
- PhD in progress : Olivier Descourbe, On Code Obfuscation, October 2016, Axel Legay and Fabrizio Biondi.
- PhD in progress : Mike Enescu, On Symbolic Execution for Malware Detection, October 2016, Axel Legay and Flavio Oquendo and Fabrizio Biondi.
- PhD in progress : Alexandre Gonsalvez, On Obfuscation via crypto primitives, April 2016, Axel Legay and Caroline Fontaine.
- PhD in progress : Nisrine Jafri (Rennes1), On fault Injection detection with MC of Binary code, December 2015, Axel Legay and Jean-Louis Lanet.
- PhD in progress : Razika Lounas, Validation des spécifications formelles de la mise à jour dynamique des applications Java Card, 2010, Mohamed Mezghiche and Jean-Louis Lanet
- PhD in progress : Aurélien Palisse, Observabilité de codes hostiles, 2015, Jean-Louis Lanet
- PhD in progress : Aurélien Trulla, Caractérisation de malware Android par suivi de flux d'information et nouvelles techniques d'évasion, 2016, Valerie Viet Triem Tong and Jean-Louis Lanet
- PhD in progress : Tristan Ninet (Rennes 1), Vérification formelle d'une implémentation de la pile protocolaire IKEv2, December 2016, Axel Legay, Romaric Maillard and Olivier Zendra

10.2.3. Juries

- Axel Legay has been a referee for the PhD defense of Najah Ben Said (University of Grenoble Alpes).
- Axel Legay has been a member of the jury for the PhD defense of Zaruhi Aslanyan (DTU Denmark).
- Jean-Louis Lanet has been a referee for the PhD defense of Pierre Belgarric (Télécom ParisTech).
- Jean-Louis Lanet has been a referee for the PhD defense of Louis Dureuil (University of Grenoble Alpes).
- Jean-Louis Lanet has been a referee for the PhD defense of Gabriel Risterucci (University of Aix Marseille).
- Jean-Louis Lanet has been a member of the jury for the PhD defense of Benoît Morgan (University of Toulouse).
- Jean-Louis Lanet has been a member of the jury for the PhD defense of Najah Ben Said (University of Grenoble Alpes).

- Olivier Zendra has been a co-referee for the PhD defense of Rabah Laouadi (University of Montpellier).

10.3. Popularization

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