



RESEARCH CENTER

FIELD

Algorithmics, Programming, Software and Architecture

Activity Report 2015

Section Dissemination

Edition: 2016-03-21

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

1. ARIC Project-Team	5
2. CAMEL Project-Team	8
3. CASCADE Project-Team	13
4. CRYPT Team	16
5. GALAAD2 Team	17
6. GEOMETRICA Project-Team	19
7. GRACE Project-Team	21
8. LFANT Project-Team	26
9. POLSYS Project-Team	30
10. SECRET Project-Team	35
11. SPECFUN Project-Team	39
12. VEGAS Project-Team	42

ARCHITECTURE, LANGUAGES AND COMPILATION

13. ALF Project-Team	45
14. ATEAMS Project-Team	48
15. CAIRN Project-Team	51
16. CAMUS Team	55
17. COMPSYS Project-Team	59
18. CORSE Team	62
19. DREAMPAL Project-Team	67
20. POSTALE Team	69
21. TASC Project-Team	71

EMBEDDED AND REAL-TIME SYSTEMS

22. AOSTE Project-Team	75
23. CONVECS Project-Team	78
24. HYCOMES Team	83
25. MUTANT Project-Team	85
26. PARKAS Project-Team	87
27. POSET Team	91
28. SPADES Project-Team	95
29. TEA Project-Team	98

PROOFS AND VERIFICATION

30. ANTIQUE Project-Team	100
31. CELTIQUE Project-Team	104
32. DEDUCTEAM Team	108
33. ESTASYS Team	110
34. GALLIUM Project-Team	111
35. MARELLE Project-Team	114
36. MEXICO Project-Team	116
37. PARSIFAL Project-Team	120

38. PIR2 Project-Team	124
39. SUMO Project-Team	128
40. TOCCATA Project-Team	131
41. VERIDIS Project-Team	137
SECURITY AND CONFIDENTIALITY	
42. CARTE Project-Team	143
43. CASSIS Project-Team	148
44. COMETE Project-Team	152
45. DECENTRALISE Team	157
46. DICE Team	158
47. PRIVATICS Project-Team	160
48. PROSECCO Project-Team	163

ARIC Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

Jean-Michel Muller was the General Chair of ARITH'22, Lyon.

10.1.1.2. Member of the organizing committees

Bruno Salvy is a co-organizer with Alin Bostan of Alea'2016, Luminy.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

Fabien Laguillaumie was a member of the program committee of WCC'15.

Benoît Libert was a member of the program committees of ACM-CCS'15, Eurocrypt'15, PKC'15 and '16, Africacrypt'16.

Jean-Michel Muller was a member of the program committee of ASAP'2015.

Nathalie Revol was a member of the program committee of NRE1 at SuperComputing'15.

Bruno Salvy is a member of program committee of AofA'2016, Warsaw, Poland.

Damien Stehlé was member of the program committees of Latincrypt'15, Asiacrypt'15, PQCrypto'16, PKC'15 and '16. He is a member of the program committee of ANTS'16 and SCN'16.

10.1.3. Journal

10.1.3.1. 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*.

Bruno Salvy is a member of the editorial boards of the *Journal of Symbolic Computation*, of the *Journal of Algebra* (section Computational Algebra) and of the collections *Texts and Monographs in Symbolic Computation* (Springer) and *Mathématiques et Applications* (SMAI-Springer).

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

10.1.4. Invited talks

Claude-Pierre Jeannerod was an invited speaker at the MACIS conference (Sixth International Conference on Mathematical Aspects of Computer and Information Sciences, Berlin, November 2015).

Damien Stehlé gave two invited talks at the HEAT workshop on fully homomorphic encryption and multilinear maps, held in Paris in October. He gave an invited talk at a Sloan Foundation workshop on the mathematics of modern cryptography, which was held in Berkeley in July. He gave two invited talks at the summer school on real-world crypto and privacy that was held in Sibenik in June.

10.1.5. 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).

Claude-Pierre Jeannerod is a member 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 general standard has been published in July 2015 (IEEE 1788-2015) and the work now addresses the set-based model (IEEE P1788.1). She was a member of a hiring committee at U. Montpellier 2 (MCF position). She is a member of the Equality-Parity Committee at Inria.

10.1.6. 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.

10.1.7. 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.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

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

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

Master: Benoît Libert, Advanced cryptographic protocols, 24h, ENS de Lyon; Computer science and privacy, 12h, ENS de Lyon; Cryptography, 12h, ENS de Lyon; Public-key cryptology, (21h), M2 ISFA (Institut de Science Financière et d’Assurances), Université Claude Bernard Lyon 1.

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

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

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

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

Master: Nicolas Louvet, *Compilation* (24h), Lyon 1.

Bachelor: Nicolas Louvet, *Algorithmique, Architecture des ordinateurs, Unix, ...*, (170h), Lyon 1.

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

Divers: Bruno Salvy, Introduction à la D-finitude (2h), *Leçons de mathématiques d’aujourd’hui*, Bordeaux.

10.2.2. Supervision

- 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: Silviu Filip, *Filtroptim : tools for an optimal synthesis of numerical filters*, since September 2013, co-supervised by Nicolas Brisebarre and Guillaume Hanrot.
- PhD in progress: 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, co-supervised by Benoît Libert (95%) and Damien Stehlé (5%).
- PhD in progress: Vincent Neiger, *Multivariate interpolation in computer algebra: efficient algorithms and applications*, since September 2013, co-supervised by Claude-Pierre Jeannerod and Gilles Villard (together with Éric Schost (Western University, London, Canada)).
- PhD in progress: Marie Paindavoine, *Méthodes de calculs sur des données chiffrées*, since October 2013 (Orange Labs - UCBL), co-supervised by Fabien Laguillaumie (together with Sébastien Canard).
- PhD in progress : Antoine Plet, *Contribution à l'analyse d'algorithmes en arithmétique virgule flottante*, since September 2014, co-supervised by Nicolas Louvet and Jean-Michel Muller.
- PhD in progress : Valentina Popescu, *Vers des bibliothèques multi-précision certifiées et performantes*, since September 2014, co-supervised by Mioara Joldes (LAAS) and Jean-Michel Muller.
- PhD in progress : Serge Torres, *Some tools for the design of efficient and reliable function evaluation libraries*, since September 2010, co-supervised by Nicolas Brisebarre and Jean-Michel Muller.
- PhD in progress: Weiqiang Wen, *Hard problems on lattices*, since September 2015, supervised by Damien Stehlé.

10.2.3. Juries

Nicolas Brisebarre was in the PhD committee of Catherine Lelay (LRI, Inria Saclay, Université Paris-Sud) and Esteban Segura Ugalde (XLIM, Université de Limoges).

Fabien Laguillaumie was in the PhD committee of Oliver Sanders (DI, ENS Paris, Orange Labs).

Benoît Libert was a reviewer and a member of the PhD committee for the PhD thesis of Olivier Sanders (DI, ENS Paris, Orange Labs).

Nathalie Revol was in the PhD committee of Qiaochu Li (Université de Technologie de Compiègne).

Bruno Salvy was a reviewer for the PhD thesis of Amaury Pouly (LIX, École polytechnique). He was in the PhD committees of Simone Naldi (LAAS, Toulouse) and Romain Serra (LAAS, Toulouse).

Damien Stehlé was a reviewer for the PhD theses of Thomas Prest (DI, ENS Paris), Zheng Wang (Imperial College, UK), Rina Zeitoun (LIP6, UPMC) and Cheng Shantian (NTU, Singapore). He is in the PhD committee of Thijs Laarhoven (TU Eindhoven, The Netherlands) and in the Habilitation thesis of Ludovic Perret (LIP6, UPMC).

10.3. Popularization

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

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

CAMEL Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

Maïke Massierer and Pierre-Jean Spaenlehauer organized a minisymposium on “Applications of polynomial system solving in cryptology”⁰ within the SIAM conference on applied algebraic geometry conference, held in Daejeon (Corea) on August 3-7, 2015.

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

- Jérémie Detrey was a member of the program committee of
 - the *Conférence d’informatique en Parallélisme, Architecture et Système* (Compas 2015);
 - the Fourth International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015).
- Pierrick Gaudry was a member of the program committee of
 - the 9th International Workshop on Coding and Cryptography (WCC 2015);
 - the 7th International Workshop on Parallel Symbolic Computation (PASCO 2015).
- Emmanuel Thomé was a member of the program committee for
 - the 19th Workshop on Elliptic Curve Cryptography (ECC 2015);
 - the 8th International Symposium on Foundations & Practice of Security (FPS 2015);
 - the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2016).
- Marion Videau was a member of the program committee of
 - the Symposium sur la sécurité des technologies de l’information et des communications, SSTIC 2015;
 - the International Conference on Information Security and Cryptology, ICISC 2015;
 - the GreHack, 2015.

10.1.2.3. Reviewing activities

- Jérémie Detrey reviewed submissions to
 - the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22);
 - the *Conférence d’informatique en Parallélisme, Architecture et Système* (Compas 2015);
 - the Fourth International Conference on Cryptology and Information Security in Latin America (Latincrypt 2015);
 - the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016).
- Pierre-Jean Spaenlehauer reviewed submissions to

⁰http://wiki.siam.org/siag-ag/index.php/Applications_of_Polynomial_System_Solving_in_Cryptology

- the 40th International Symposium on Symbolic and Algebraic Computations (ISSAC 2015);
- the 21st Annual Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2015);
- 6th International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS 2015);
- The 28th International Conference of the Jangjeon Mathematical Society (ICJMS 2015).
- Maïke Massierer reviewed a submission to the IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2015).
- Pierrick Gaudry reviewed submissions to
 - the 30th ACM/SIGAPP Symposium On Applied Computing (SAC 2015);
 - the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22);

10.1.3. Journal

10.1.3.1. Member of the editorial boards

- Pierrick Gaudry is a member of the editorial board of *Applicable Algebra in Engineering, Communication and Computing* (AAECC).

10.1.3.2. Reviewing activities

- Jérémie Detrey reviewed submissions to
 - the IEEE Transactions on Dependable and Secure Computing (TDSC);
 - the ACM Transactions on Mathematical Software (TOMS).
- Pierre-Jean Spaenlehauer reviewed submissions to
 - the Journal of Symbolic Computation (JSC);
 - *Commentationes Mathematicae Universitatis Carolinae* (CMUC);
 - *Mathematical Modeling and Numerical Analysis* (ESAIM-M2AN);
 - the Journal of Cryptographic Engineering (JCEN).
- Maïke Massierer reviewed submissions to
 - *Finite Fields and Applications* (FFA);
 - *Applicable Algebra in Engineering, Communication and Computing* (AAECC).
- Pierrick Gaudry reviewed submissions to
 - *Applicable Algebra in Engineering, Communication and Computing* (AAECC).
 - *Journal of Cryptology*;

10.1.4. Invited talks

- Jérémie Detrey gave invited talks at
 - the tutorial session of the 22nd IEEE Symposium on Computer Arithmetic (ARITH 22, June, Lyon, France);
 - the summer school of the 19th Workshop on Elliptic Curve Cryptography (ECC 2015, September, Bordeaux, France).
- Pierre-Jean Spaenlehauer gave invited talks at
 - the Workshop on Structured Low-Rank Approximation (June, Grenoble, France);
 - the SIAM conference on Applied Algebraic Geometry, Minisymposium on Algorithms and Complexity in Polynomial System Solving (August, Daejeon, Korea);
 - the SIAM conference on Applied Algebraic Geometry, Minisymposium on ML Degree and Critical Points (August, Daejeon, Korea);

- the Third Workshop on Hybrid Methodologies for Symbolic-Numeric Computations (August, Beijing, China);
- the Workshop on Algebra, Geometry and Proofs in Symbolic Computation (December, Toronto, Canada).
- Pierrick Gaudry gave invited talks at
 - the CATREL Workshop: Advances in Discrete Logarithms (October, Palaiseau, France);
 - the Colloquium Jacques Morgenstern (Nice-Sophia).
- Emmanuel Thomé gave an invited talk at the CATREL Workshop: Advances in Discrete Logarithms (October, Palaiseau, France).

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.
- Pierre-Jean Spaenlehauer is a member of the *Commission des développements technologiques* (CDT) of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry was a member in 2015 of
 - the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
 - the hiring committee for an associate professor position Univ. Montpellier;
 - the committee for the HCERES evaluation of the LITIS laboratory in Rouen;
 - the evaluation committee for the *Algorithmics, Computer Algebra and Cryptology* Inria theme, acting as *coordinator*.
- 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.
- Marion Videau was a member of the hiring committee for the 2015 junior research positions (CR2) at Inria Saclay.
- Laurent Grémy is a member of the *Conseil de laboratoire* of the Loria.

10.1.6. Seminar organisation

10.1.6.1. CAMEL seminar

Five speakers were invited in our seminar in 2015: Matthieu Rambaud, Roland Wen, Jan Tuitman, Frédéric Bihan, Chenqi Mou.

10.1.6.2. Joint security seminar with the university master in computer science

The team is involved with other teams and the university master in computer science in the organization of the security seminar which started in 2013. Fifteen speakers were invited in 2015: Graham Steel, Nicolas Fischbach, Georges Bossert, Jean-Philippe Aumasson, Khartik Bhargavan, Kenny Paterson, Bertrand Wallrich, Cédric Lauradoux, Nora Cuppens, Christian Grothoff, Éric Freyssinet, Maxime Clementz, Kostas Chatzikokolakis, Emmanuel Thomé, Olivier Levillain.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence

Jérémy Detrey, *Security of websites*, 2 hours (lecture), L1, Université de Lorraine, IUT Charlemagne, Nancy, France.

Jérémy Detrey, *Introduction to Cryptology and Information Security*, 10 hours (lectures) + 10 hours (tutorial sessions) + 10 hours (practical sessions), L3, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Pierrick Gaudry, *Algorithmique et Programmation*, 16 hours (practical sessions), L1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

Master

Pierre-Jean Spaenlehauer, *Introduction to Cryptography*, 12 hours (lectures), M1, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Emmanuel Thomé, *Introduction to Cryptography*, 12 hours (lectures), M1, Télécom Nancy, Vandœuvre-les-Nancy, France.

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

Marion Videau and Stéphane Glondu supervised the semestrial project of all the students of M2, SSSR-SAW, Université de Lorraine, département d'informatique, France.

Other

Emmanuel Thomé, *Discrete logarithms in Finite Fields*, advanced course for the ECC 2015 summer school, Bordeaux, France.

10.2.2. Supervision

- **Ph.D. in progress**

Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, since Sep. 2015, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

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

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

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

- **Ph.D. defended in 2015**

Cyril Bouvier, *Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret*, supervised by Paul Zimmermann, defended in June.

Hamza Jeljeli, *Accélérateurs logiciels et matériels pour l'algèbre linéaire creuse sur les corps finis*, supervised by Jérémy Detrey & Emmanuel Thomé, defended in July.

10.2.3. Juries

- Jérémy Detrey was a member of the jury of the ÉNS competitive entrance exam.

- Pierrick Gaudry was a reviewer and member of the jury for the PhD thesis of Enea Milio (Univ. Bordeaux); he was in the jury for the PhD thesis of Florent Rovetta (Univ. Aix-Marseille).
- Emmanuel Thomé was a reviewer and member of the jury for the PhD thesis of Bastien Violla (Montpellier).
- Marion Videau was a reviewer and member of the jury for the PhD thesis of Stéphanie Riaud (Rennes).

10.3. Popularization

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

CASCADE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Organisation of Events

- a weekly seminar is organized: <http://www.di.ens.fr/CryptoSeminaire.html>
- monthly working group on lattices, joint with ENS Lyon
- Organization of the *Summer School on Mathematical and Practical Aspects of Fully Homomorphic Encryption and Multi-Linear Maps* at IHP, Paris, in October 2015 (supported by CryptoAction, SAFEcrypto, CryptoCloud, and aSCEND)

8.1.1.2. Steering Committees of International Conferences

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

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 serves on the committee and has even been elected as 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 Member

- PKC 2015 – March 30 - April 1 (Maryland, USA): Michel Abdalla
- CT-RSA – 20-25 April (San Francisco, California, USA): David Pointcheval
- Eurocrypt – 26-30 April (Sofia, Bulgaria): David Pointcheval
- ACNS – 2-5 June (New-York, USA): David Pointcheval
- CRYPTO – 16-20 Aug (Santa Barbara, California, USA): Michel Abdalla
- LATINCRYPT – 23-26 Aug (Guadalajara, Mexico): Michel Abdalla
- IWSEC – 26-28 Aug (Nara, Japan): Damien Vergnaud
- FOCS – 18-20 Oct (Berkeley, California, USA): Hoeteck Wee
- ProvSec – 24-26 Nov (Kanazawa, Japan): Michel Abdalla, Damien Vergnaud

8.1.2.2. Funding Panel and Committee Member

- ANR – Scientific Evaluation Panel « Global Security and Cybersecurity »: Damien Vergnaud

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 *Security and Communication Networks*: David Naccache (editor)
- of *Journal of Cryptographic Engineering*: David Naccache (editor)
- of *Computers & Security* – Elsevier: David Naccache
- of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla
- of *IET Information Security*: Michel Abdalla
- of *ETRI Journal*: Michel Abdalla

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, Vadim Lyubashevsky, Cryptography, M2, MPRI
- Master: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: David Pointcheval, Cryptography, M2, ESIEA

8.2.2. Supervision

- PhD: Sylvain Ruhault, Security Analysis of Pseudo Random Generators, ENS, June 30th, 2015, David Pointcheval & Damien Vergnaud
- PhD: Olivier Sanders, Conception et Optimisation de Mécanismes Cryptographiques Anonymes, ENS, September 24th, 2015, David Pointcheval
- PhD: Sonia Belaïd, Security of Cryptosystems Against Power-Analysis Attacks, ENS, October 22nd, 2015, Michel Abdalla
- PhD: Thomas Prest, Gaussian Sampling in Lattice-Based Cryptography, ENS, December 8th, 2015, Vadim Lyubashevsky
- PhD: Diana Maimut*, Authentication and Encryption Protocols: Design, Attacks and Algorithmic Improvements, ENS, December 11th, 2015, David Naccache
- PhD in progress: Fabrice Ben Hamouda, Leakage of information in cryptography, from 2012, Michel Abdalla & David Pointcheval
- PhD in progress: Jérémie Clément*, Lightweight cryptography, from 2013, David Naccache
- PhD in progress: Simon Cogliani*, Authenticated Encryption, from 2013, David Naccache
- PhD in progress: Mario Cornejo, Security for the cloud, from 2013, Michel Abdalla
- PhD in progress: Houda Ferradi*, Biometric protocols and mobile security, from 2013, David Naccache
- PhD in progress: Alain Passelègue, Security against related-key attacks, from 2013, Michel Abdalla
- PhD in progress: Adrian Thillard, Counter-measures against side-channel attacks and secure multi-party computation, from 2013, Damien Vergnaud
- PhD in progress: Raphael Bost, Symmetric Searchable Encryption, from 2014, David Pointcheval
- PhD in progress: Florian Bourse, Encryption Schemes for the Cloud, from 2014, Michel Abdalla & David Pointcheval
- PhD in progress: Geoffroy Couteau, Efficient secure two-party computation for the Cloud, from 2014, David Pointcheval & Hoeteck Wee

- PhD in progress: Rafael Del Pino, Lattice-Based Cryptography – Complexity and Ideal-Lattices, from 2014, Vadim Lyubashevsky
- PhD in progress: Rémi Géraud*, Provable security in public-key cryptography, from 2014, David Naccache
- PhD in progress: Pierrick Meaux, Lattice-Based Cryptography – Advanced Features, from 2014, Vadim Lyubashevsky
- PhD in progress: Thierry Mefenza Nountu, Number-Theoretic Study of Pseudorandom Cryptographic Primitives, from 2014, Damien Vergnaud
- 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

* Since David Naccache left the team, these students also moved in his new Security team.

8.2.3. Juries

- HdR Benoît Libert. *Applications of Structure-Preserving Cryptography and Pairing-Based NIZK Proofs* – ENS Lyon – France, April 29th, 2015: David Pointcheval (reviewer)
- PhD Sylvain Ruhault. *Security Analysis of Pseudo Random Generators* – ENS – France, June 30th, 2015: David Pointcheval & Damien Vergnaud (supervisors)
- PhD Olivier Sanders. *Conception et Optimisation de Mécanismes Cryptographiques Anonymes* – ENS – France, September 24th, 2015: David Pointcheval (supervisor), Michel Abdalla
- PhD Sonia Belaïd. *Security of Cryptosystems Against Power-Analysis Attacks* – ENS – France, October 22nd, 2015: Michel Abdalla (supervisor)
- PhD Thomas Prest. *Gaussian Sampling in Lattice-Based Cryptography* – ENS – France, December 8th, 2015: Vadim Lyubashevsky (supervisor), David Pointcheval
- PhD Diana Maimut. *Authentication and Encryption Protocols: Design, Attacks and Algorithmic Improvements* – ENS – France, December 11th, 2015: David Naccache (supervisor), David Pointcheval
- PhD Bastien Vialla. *Contributions to Exact Linear Algebra over Finite Fields and Homomorphic Encryption* – Montpellier – France, December 14th, 2015: Damien Vergnaud (reviewer)

CRYPT Team

6. Dissemination

6.1. Promoting Scientific Activities

6.1.1. Scientific events selection

6.1.1.1. Reviewer

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

6.1.2. Journal

6.1.2.1. Member of the editorial boards

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

6.1.2.2. Reviewer - Reviewing activities

The members of the team reviewed numerous papers for numerous journals.

6.1.3. Invited talks

Phong Nguyen gave several invited talks:

- [13] at the Workshop on the Mathematics of Lattices and Cybersecurity, at ICERM in the USA.
- at the Workshop on cryptography based on elliptic curves and lattices, organized by Beijing University in China.

6.1.4. Research administration

Phong Nguyen was the European director of LIAMA until Oct. 2015, and is now the French director of JFLI (Japanese-French Laboratory for Informatics).

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

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

6.2.2. Supervision

PhD: Jiangwei Li, Several Computational Problems in Lattice Theory, Tsinghua, June 2015, Xiaoyun Wang

PhD: Dan Ding, y -Sparse Representations of Short Lattice Vectors and Algorithms for the Shortest Vector Problem (SVP) in Lattices, Tsinghua, June 2015, Xiaoyun Wang

PhD: Gengran Hu, On Lattice Theory and Complexity of SVP, CAS, Summer 2015, Yanbin Pan

PhD: Chang Lv, Primality tests, ring class fields and Diophantine equations, CAS, Summer 2015, Yingpu Deng

PhD: Dandan Huang, primality tests for numbers and ideals, CAS, Summer 2015, Yingpu Deng

6.2.3. Juries

PhD: Rina Zeitoun, Algebraic Methods for the Security Analysis of Cryptographic Algorithms Implementations, University Paris 6 (UPMC), July 2015, Phong Nguyen (Jury member)

GALAAD2 Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

8.1.1.1. Member of the conference program committees

Evelyne Hubert, André Galligo and Bernard Mourrain were part of the selection committee for the conference MEGA that took place in Trento (Italy) in June.

8.1.1.2. Reviewer

Laurent Busé wrote reviews for the conference ISSAC (International Symposium in Symbolic and Algebraic Computation), Bath, UK, July.

Bernard Mourrain was reviewer for the conferences MEGA (Effective Methods in Algebraic Geometry), Trento, Italy, June, ISSAC (International Symposium in Symbolic and Algebraic Computation), Bath, UK, July.

8.1.2. Journal

8.1.2.1. Member of the editorial boards

Evelyne Hubert and Bernard Mourrain are associate editors of the Journal of Symbolic Computation (since 2007).

8.1.2.2. Reviewer - Reviewing activities

Laurent Busé wrote reviews for the following journals: Graphical Models, IEEE Transactions on Visualization and Computer Graphics, Computer Aided Geometric Design, Journal of Algebra, Journal of Symbolic Computation, Math. Zeitschrift, Mathematical Problems in Engineering, Applicable Algebra in Engineering Communication and Computing, Applied Mathematics and Computation. He also reviewed a research proposal for the Austrian Science Fund (FWF).

Evelyne Hubert reviewed articles for the Journal of Symbolic Computation, Mathematics of Computation, Acta Applicandae Mathematicae, and the Journal of Mathematical Analysis and Applications.

Bernard Mourrain reviewed articles for Applied Numerical Mathematics journal, Computer Aided Geometric Design journal, Computing Surveys, Journal of Symbolic Computation, Journal of Pure and Applied Algebra, Reliable Computing, SIAM Journal on Matrix Analysis and Applications, SIAM Journal on Optimization, Transactions on Mathematical Software.

8.1.3. Invited talks

Evelyne Hubert was invited to give colloquium talks at the Aalto Science Institute (Finland) in April and at the department of mathematics of the University of Western Ontario (Canada) in november. She was also invited to give a talk at the *Workshop on Symbolic Combinatorics and Computational Differential Algebra* that took place in September at the Fields institute in Toronto (Canada).

Bernard Mourrain was an invited speaker of the Algebra and Geometry Meeting, Universitat de Barcelona, 2-5 December.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

Master: Bernard Mourrain, Real effective algebraic geometry, 30h, M2 Mathématiques, Univ. 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: Mathieu Collowald, Integral representation of shapes for feature conservation or extraction, started in 2011, supervised by Evelyne Hubert.

8.2.3. Juries

Laurent Busé was part of the PhD jury of José Naéliton da Silva (residual intersections and annihilators of Koszul homologies) at IMPA, Rio de Janeiro, April 13.

Evelyne Hubert was part of the PhD juries of Romain Casati (modélisation numérique de structures élançées pour l'informatique graphique) from University of Grenoble, of Romain Basson (Arithmétique des espaces de modules des courbes hyperelliptiques de genre 3 en caractéristique positive) from University of Rennes, of Mathieu Collowald (Multivariate moment problems: applications of the reconstruction of linear forms on the polynomial ring) Inria, Sophia Antipolis, defended in December.

Bernard Mourrain was member of the PhD juries of Esteban Segura Ugalde (Computation of Invariant Pairs and Matrix Solvents) University of Limoges, defended in June; of Simone Naldi (Exact algorithms for determinantal varieties and semidefinite programming) LAAS, Toulouse, defended in September; of Mathieu Collowald (Multivariate moment problems: applications of the reconstruction of linear forms on the polynomial ring) Inria, Sophia Antipolis, defended in December.

Bernard Mourrain was member of the Jury for Inria CR2 positions at the center of Inria Rhône-Alpes, Grenoble.

GEOMETRICA Project-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 20-24.
- Frédéric Chazal co-organised the Focused program on “Functoriality in Geometric Data” at the Institute for Advanced Study, HKUST Hong-Kong, April 2015.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

Frédéric Chazal: Geometric Science of Information 2015 (GSI 2015).

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, Algorithmica, 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, Graphical Models*.

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

10.1.4. Invited talks

Frédéric Chazal, Focused program on “Functoriality in Geometric Data”, Institute for Advanced Study, HKUST Hong-Kong, April 2015.

Frédéric Chazal, Geometry and Data Analysis conference, Stevanovich Center for financial mathematics, University of Chicago, June 2015.

Frédéric Chazal, Mini-conference on Topological Data Analysis, Oxford University, June 2015.

Frédéric Chazal, European Meeting of Statisticians (EMS 2015), Amsterdam, July 2015.

Frédéric Chazal, 2nda Escuela/Conferencia de Análisis Topológico de Datos, Queretaro, Mexico, December 2015

Steve Oudot, *GETCO (Applications of Algebraic Topology in Computer Science and Data Analysis)*, Aalborg, April 2015.

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

Master : S. Oudot, *Topological Data Analysis*, 36h, École polytechnique.

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

Master : J.D. Boissonnat, *Winter School : "Algorithmic Geometry of Triangulations"*, January 2015.

Master : S. Oudot, *Summer School BioMed : "Topological Descriptors for Geometric Data Comparison"*, July 2015.

Master : S. Oudot, *Young Researchers School at the Journées de l'AFIG : "Topological Methods for 3D Processing"*, November 2015.

Doctorat : Frédéric Chazal, *Topology and Geometry of Data Analysis*, 9h eq-TD, nd EATCS Young Researchers School and TopDrim School "Understanding Complexity and Concurrency through Topology and Data", Camerino, Italy, July 2015.

10.2.2. Supervision

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

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

PhD in progress : Siargey Kachanovich : *Manifold Learning*, started October 2015. Jean-Daniel Boissonnat

PhD in progress: Thomas Bonis, *Statistical Learning Algorithms for Geometric and Topological Data Analysis*, started December 1st, 2013, Frédéric Chazal.

PhD in progress: Ruqi Huang, *Algorithms for topological inference in metric spaces*, started December 1st, 2013, 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: Jérémy Cochoy, *Zigzag persistence: stability and applications to Topological Data Analysis*, started September 1st, 2015, Steve Oudot (co-advised by F. Chazal).

PhD in progress: Mathieu Carrière, *Signatures for Geometric Shapes*, started September 1st, 2014, Steve Oudot.

10.2.3. Juries

Jean-Daniel Boissonnat was a member of the HDR defense committee of Quentin Mérigot (Université de Grenoble).

Frédéric Chazal was a member of the HDR defense committee of Bertrand Michel (Université Pierre et Marie Curie).

Frédéric Chazal was a member (and reviewer) of the PhD defense committee of Julien André (Université Grenoble).

Frédéric Chazal was a member of the PhD defense committee of Stéphane Calderon (Telecom Paris).

Frédéric Chazal was a member of the PhD defense committee of Fabrizio Lecci (Carnegie Mellon University).

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.
- A. Couvreur organized with David Kohel (I2M, Marseille) and Alp Bassa (Bogazici University, Turkey) the conference AGC²T 15 (Arithmetic Geometry, Cryptography, and Coding Theory) at CIRM (Marseille). This 15th edition of this international conference happened from May 18 to 22, 2015.
- F. Morain, B. Smith and A. Guillevic were the organizers of **Advances in Discrete Logarithms**, an international workshop on discrete logarithms to conclude the CATREL project, at École polytechnique from October 1 to 2, 2015.
- P. Lebacque and B. Smith organized **Arithmetic Geometry: Explicit Methods and Applications** with C. Ritzenthaler and A. Zykin. This was an international number theory conference, held in Moscow from December 7 to 11, 2015.
- A. Guillevic and P. Karpman were members of the local organizing team of CHES 2015 (Cryptographic Hardware and Embedded Systems), at Saint-Malo, France, in September.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

- A. Couvreur was member of the program committee of *Journées Codes et Cryptographie 2015*, La Londe les Maures. October 2015.
- A. Couvreur was member of the program committee of WCC (Workshop on Codes and Cryptology) 2015. Paris, May 2015.
- A. Couvreur was member of the scientific committee of the *École Mathématique Africaine: Théorie des nombres et Cryptologie, Équations aux dérivées partielles, analyse numérique et calcul scientifique*. March 2015, Franceville (Gabon).

10.1.2.2. Reviewer

- D. Augot was reviewer for
 - ISIT 2015 (International Symposium on Information Theory)
 - CAI 2015 (6th International Conference on Algebraic Informatics)
 - SODA 2016 (Symposium on Discrete Algorithms)
- A. Couvreur was reviewer for
 - PQCrypto 2016.
- P. Karpman was reviewer for
 - ACNS 2015
 - CRYPTO 2015
 - ASIACRYPT 2015
 - INDOCRYPT 2015
 - EUROCRYPT 2016

- FSE 2016
- B. Smith was a reviewer for
 - MEGA 2015
 - PKC 2015
 - EUROCRYPT 2016

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.

10.1.3.2. Reviewer - Reviewing activities

- D. Augot was a reviewer for
 - Designs, Codes and Cryptography
 - IEEE Transactions on Information Theory
 - Discrete Mathematics
 - Transactions on Computers
 - Applicable Algebra in Engineering, Communication and Computing
 - Advances in Mathematics of Communications
 - Ars Comb
- A. Couvreur was reviewer for
 - Finite Fields Appl.
 - Des. Codes Cryptogr.
 - Mosc. Math. J.
 - J. Numbers.
- B. Smith was a reviewer for
 - Journal of Cryptology
 - SICOMP (SIAM Journal on Computing)

10.1.4. Invited talks

- D. Augot was invited to the colloquium of IRMAR, Rennes
- D. Augot was invited to the workshop "Codage et cryptographie", USTHB, Algiers, November 2-5.
- A. Couvreur was invited at the seminar of number theory of University of Oxford.
- A. Couvreur was invited speaker at the conference *Arithmetic Geometry: explicit methods and applications*, Moscow, december 2015.
- A. Guillevic was invited at the Workshop in Elliptic Curve Cryptography (ECC), Bordeaux, September 2015.
- A. Guillevic was invited at the CATREL Workshop on Discrete Logarithms organized by the GRACE team at Palaiseau, October 2015.
- P. Karpman was invited at the RISC seminar of CWI, Amsterdam.
- B. Smith was an invited speaker in the LFANT seminar, Bordeaux, February 2015
- B. Smith was an invited speaker in the security seminar at University College London, UK, May 2015

- B. Smith was an invited speaker at the Colóquio de Geometria e Aritmética (Geometry and Arithmetic Colloquium) at IMPA, Rio de Janeiro, Brazil, October 2015
- B. Smith gave an invited Tech Talk at Cisco France, Paris, November 2015
- B. Smith gave an invited talk in the cryptography and security seminar at Radboud University Nijmegen, Netherlands, December 2015

10.1.5. Leadership within the scientific community

Together with Inria Nancy Caramel team, we are leader on records discrete logarithms, thanks to the CATREL project, which delivered the CADO-NFS software, and to our experience to run hard computational projects to achieve these records. We have also proposed the best curves for cryptographic computations.

10.1.6. Scientific expertise

- D. Augot explained the fundamental concepts underlying bitcoin to the “Direction de la prospective de la Poste”

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 *conseil de laboratoire*
- D. Augot is elected member of the *conseil académique consultatif* of Paris-Saclay University.
- B. Smith was a reviewer for ANRT CIFRE funding.
- F. Morain and B. Smith are elected members of the *Conseil de Laboratoire* of the LIX.
- F. Morain is vice-head of the Département d’informatique of Ecole Polytechnique.
- F. Morain represents École polytechnique in the committee in charge of *Mention HPC* in the *Master de l’université Paris Saclay*.
- 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.

Juries

- D. Augot was in committee assessing candidates for Institut Mines-Télécom.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence

A. Couvreur, INF311: “Introduction à l’informatique”, 40h (equiv TD), L3, École polytechnique, France

A. Couvreur INF411: “Les bases de la programmation et de l’algorithmique”, 32h (equiv TD), M1, École polytechnique, France

F. Levy-dit-Vehel, “Cours de Cryptographie”, 30h. (equiv TD), 3rd year (M1), ENSTA ParisTech, France.

F. Levy-dit-Vehel, “Mathématiques discrètes pour la protection de l’information”, 24h (equiv TD), 2nd year (L3), ENSTA ParisTech, France.

F. Morain, Lectures for INF311: “Introduction à l’informatique”, 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).

B. Smith, INF442: “Traitement des données massives”, 32h (equiv TD), L4, École polytechnique, France

Master

A. Couvreur, “Error-correcting codes and applications to cryptography”, 12h (equiv TD), M2, MPRI, France.

F. Morain, “Algorithmes arithmétiques pour la cryptologie”, 9h (equiv TD), M2, MPRI, France.

F. Morain, Lectures for INF568: “Cryptology”, 13.5h (equiv TD), 3rd year (M1), École polytechnique, France.

B. Smith, “Algorithmes arithmétiques pour la cryptologie”, 13.5h (equiv TD), M2, MPRI, France.

B. Smith, Cryptologie, 18h (equiv TD), M1, École polytechnique, France

10.2.2. Supervision

- PhD: G. Robert defended his thesis on December 4th, 2015 [12].
- PhD in progress. J. Lavauzelle has began his Ph.D. on locally decodable codes and cryptogra[phic 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.
- PhD in progress. P. Karpman, starting in 2013, will defend in 2016 his PhD on security of symmetric cryptographic primitives.

10.2.3. Juries

- D. Augot was reviewer of
 - J. Roué PhD thesis, “Analyse de la résistance des chiffrements par blocs aux attaques linéaires et différentielles”, Université Pierre et Marie Curie
 - F. de Portzamparc PhD thesis, “Algebraic and Physical Security in Code-Based Cryptography”, Université Pierre et Marie Curie
- A. Couvreur
 - was reviewer of F. de Portzamparc PhD thesis, “Algebraic and Physical Security in Code-Based Cryptography”, Université Pierre et Marie Curie
 - is member of the Jury of Agrégation de Mathématiques and in charge of option C (*Algèbre et calcul formel*)

- B. Smith
 - was an examiner for L. Xu’s PhD thesis, “Vérification formelle de la vie privée dans les systèmes concurrents”, École polytechnique, 4/5/2015.

10.3. Popularization

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

10.4. Institutional commitment

- F. Levy-dit-Vehel is member of ENSTA ParisTech working group “compétences et validation des acquis de l’expérience”.
- B. Smith was “responsable des bureaux” (responsible for allocating desks and offices) at LIX.

LFANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

The team has organised the international conference ECC 2015 — 19th Workshop on Elliptic Curve Cryptography in Bordeaux from September 28 to September 30 and a Summer School on elliptic curves the week before from September 23 to September 25.

The three day conference with 170 participants comprised about fifteen invited lectures by world-renowned scientist, presenting the major advances of the previous year. Topics ranged widely from new mathematical and algorithmic results on elliptic curves and abelian varieties, over implementations and attacks of cryptosystems up to practical studies on real-world use of curve based cryptography. This year, a panel discussion on the standardisation of elliptic curves for cryptographic use was also organised.

The preceding summer school with about 70 participants included four invited lectures of three hours each (one of which was given by Damien Robert), and a software tutorial on Sage and Pari/GP. The tutorial on Pari/GP was done by Bill Allombert and Karim Belabas. The school concluded with an afternoon of computer exercises.

8.1.1.1. General chair, scientific chair

Andreas Enge and Damien Robert were scientific chairs, Andreas Enge was the general chair.

8.1.1.2. Member of the organizing committees

Andreas Enge, Anne-Laure Gautier and Damien Robert were members of the organizing committee.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committees

- Andreas Enge was the programme chair of ECC 2015 (Bordeaux)

8.1.2.2. Member of the conference program committees

- Damien Robert was a member of the ECC 2015 (Bordeaux), Asiacrypt 2015 (Auckland) and CRI 2015 (Yaoundé) program committees.
- Sorina Ionica was a member of the Latincrypt 2015 (Guadalajara, Mexico) program committee.

8.1.3. Journal

8.1.3.1. 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.

8.1.4. Invited talks

- F. Johansson gave an invited talk on "Fast arbitrary-precision evaluation of special functions in the Arb library" at The 13th International Symposium on Orthogonal Polynomials, Special Functions and Applications (OPSFA-13), National Institute of Standards and Technology, Gaithersburg, MD, USA (June 2015)
- S. Ionica gave an invited talk on "Fast scalar multiplication in pairing groups" at the "Pairings in cryptography" Minisymposium, SIAM AG15 Conference, Daejeon, South Korea (August 2015)
- A. Enge gave an invited talk on "Computing with theta functions on abelian surfaces" at the 11th Symposium on Algebra and Computation (AC2015), Tokyo Metropolitan University (December 2015)
- E. Milio gave an invited talk on "Computation of modular polynomials in dimension 2" at the Elliptic Curve Cryptography 2015 Conference in Bordeaux (September 2015). He also gave a similar talk at the Journées codage et cryptographie at la Londe-les-Maures (October 2015).
- D. Robert gave two invited talks on "Isogenies, Polarizations and Real Multiplication", one for the Modular Forms and Curves of Low Genus: Computational Aspects conference at Providence (September 2015) and one for the Journées codage et cryptographie at la Londe-les-Maures (October 2015).

8.1.5. 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.

8.1.6. Research administration

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 Universités" (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).

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: Enea Milio, Analyse, 12h, L1, Université de Bordeaux, France;

Licence: Enea Milio, Mise à niveau Maths, 12h, L1, Université de Bordeaux, France;

Licence: G. Castagnos, *Algorithmique algébrique 1*, 34.67h, L3, University of Bordeaux, France

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*, 30h, M2, University of Bordeaux, France;

Master: K. Belabas, *Computational number theory*, 70h, M2, University of Bordeaux, France;

Master: K. Belabas, *Computer Algebra*, 90h, M2, University of Bordeaux, France;

Master: K. Belabas, *Algorithms for Public Key Cryptography*, 30h, M2, University of Bordeaux, France;

Summer School: F. Johansson gave three invited lectures on "High-precision methods for zeta functions" at the UNCG Summer School in Computational Number Theory, Greensboro, NC, USA in May 2015;

Summer School: J.-M. Couveignes and D. Robert gave a one week course on *Algorithmic number theory and cryptology* for the École Mathématique Africaine, organised with support from the Centre International de Mathématiques Pures et Appliquées (CIMPA) in March 2015 at Franceville, Gabon.

Summer School: D. Robert gave a talk on *The group structure of rational points of elliptic curves over a finite field* (including practical exercises on Sage or Pari/GP) for the Elliptic Curves Cryptography (ECC 2015) Summer School in September 2015 at Bordeaux.

Summer School: D. Robert gave a one week course on *Introduction to cryptology* as part of the seminar on security at Yaoundé I University preceding the Colloque de Recherche en Informatique in December 2015.

Summer School: S. Ionica gave a two lecture course on *Introduction to elliptic curve cryptography* at the ASCrypto 2015, the summer school organised at the Latincrypt 2015 conference, in Guadalajara, Mexico.

Summer School: A. Enge gave eight lectures at the SEAMS school on *Algebras and their applications (Quantum Physics, Cryptography and Statistics)* at Universiti Putra Malaysia in November 2015, entitled *Elliptic curves* (two lectures), *Hyperelliptic curves* (two lectures), *Kummer varieties*, *Exponential and subexponential algorithms for the discrete logarithm problem* (two lectures), *Pairings on elliptic curves*.

8.2.2. Supervision

PhD: Athanasios Angelakis, *Universal Adelic Groups for Imaginary Quadratic Number Fields and Elliptic Curves*, University of Bordeaux / University of Leiden, supervised by K. Belabas and P. Stevenhagen, defended 09/2015.

PhD: Julio Brau, *Galois representations of elliptic curves and abelian entanglements*, University of Bordeaux / University of Leiden, supervised by K. Belabas and P. Stevenhagen, defended 12/2015.

PhD: Enea Milio, *Computing modular polynomials in dimension 2*, University Bordeaux, supervised by A. Enge and D. Robert, defended 12/2015.

PhD in progress: Iuliana Ciocanea, *The module isomorphism problem*, supervised by K. Belabas and H. Lenstra.

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

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

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

F. Johansson was a mentor in Google Summer of Code for Anubhav Srivastava (undergraduate student at IIIT Hyderabad) who did a successful GSoC project on "BLAS wrappers for linear algebra in FLINT"

S. Ionica supervised P. Bert's Master 1 thesis "Index calculus algorithms for small genus hyperelliptic curves". P. Bert is a student of the CSI master (Univ. of Bordeaux) and was an intern with LFANT from the 10th of May 2015 to the 31th of July 2015.

8.2.3. Juries

K. Belabas was a member of the jury of Olga Balkanova's PhD defense in Bordeaux (supervised by G. Molteni and G. Ricotta)

K. Belabas was a member (as supervisor) of the juries of Athanasios Angelakis and Julio Brau.

J.-M. Couveignes was a member of the jury, as a referee, for François Arnaud's HDR defense.

J.-M. Couveignes was a member of the jury, for Cyril Bouvier's PhD defense.

J.-M. Couveignes was a member of the jury, for Tristan Vaccon's PhD defense.

J.-M. Couveignes was a member of the jury, for Kevin Atighehchi's PhD defense.

A. Enge and D. Robert were members (as supervisors) of the jury for Enea Milio's PhD defense.

8.3. Popularization

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

POLSYS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

Guénaél Renault and Emmanuel Prouff were both General Co-chairs of CHES 2015.

9.1.1.2. Member of the organizing committees

Dongming Wang was involved in the organization of the following conferences

- Fourth International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2015) (Beijing, China, October 21-23, 2015);
- Dagstuhl Seminar 15471: Symbolic Computation and Satisfiability Checking ((SC)² 2015) (Dagstuhl, Germany, November 15-20, 2015);
- International Seminar on Geometric Computation (GC 2015) (Nanning, China, February 2-4, 2015).

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

Dongming Wang was Program Co-chair of the following conferences

- Fourth International Seminar on Program Verification, Automated Debugging and Symbolic Computation (PAS 2015) (Beijing, China, October 21-23, 2015);
- Dagstuhl Seminar 15471: Symbolic Computation and Satisfiability Checking ((SC)² 2015) (Dagstuhl, Germany, November 15-20, 2015);
- International Seminar on Geometric Computation (GC 2015) (Nanning, China, February 2-4, 2015).

9.1.2.2. Member of the conference program committees

Jean-Charles Faugère was member of the program committees of the following conferences

- PKC 2015
- Eurocrypt 2016

Ludovic Perret was member of the program committees of the following conferences

- The 7th International Workshop on Parallel Symbolic Computation (PASCO'15)
- The 41th International Symposium on Symbolic and Algebraic Computation (ISSAC'16)

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

- Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015);
- 14th Smart Card Research and Advanced Application Conference (CARDIS 2015);
- 6th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE);
- Indocrypt 2015.

Guénaél Renault was member of the program committees of the following conferences

- International Symposium on Symbolic and Algebraic Computation (ISSAC 2015)

Mohab Safey El Din was member of the program committees of the following conference

- International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2015;

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

- International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS);
- International Symposium on Symbolic Computation in Software Science (SCSS).

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.

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

Jean-Charles Faugère was invited speaker at

Workshop on “Grobner bases techniques for post-quantum cryptography”, March 27, 2015 Washington (USA)

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Sixth International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) Nov 11–13, 2015 Zuse Institute Berlin (ZIB), Germany.

Journées Nationales de Calcul Formel (3 hours lecture) Oct 2015, Cluny France

Daniel Lazard was special invited talk at Effective Methods in Algebraic Geometry 2015 - Università di Trento, Trento, June 2015.

Emmanuel Prouff was invited talk at Workshop on Constructive Side-Channel Analysis and Secure Design 2015, Mövenpick Hotel, Berlin, Apr. 2015.

Mohab Safey El Din was invited speaker at

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Workshop on Linear Computer Algebra and Symbolic-Numeric Computation, Thematic Program on Computer Algebra, Fields Inst. Toronto, Oct. 2015.

Workshop Algebraic Vision, TU Berlin, October 2015.

Dagstuhl seminar on Complexity of Symbolic and Numeric Procedures, Dagstuhl, Germany, June 2015.

Czech workshop on applied mathematics in engineering Prague, Czech, February, 2015.

Mohab Safey El Din was also invited to give talks at

Minisymposium on Maximum Likelihood Degrees and Critical Points, SIAM Conference on Applied Algebraic Geometry, Daejeon, Aug. 2015, South-Korea.

Minisymposium on Real algebraic geometry and Optimization, SIAM Conference on Applied Algebraic Geometry, Daejeon, Aug. 2015, South-Korea.

Minisymposium on Polynomial Optimization and Moments, SIAM Conference on Applied Algebraic Geometry, Daejeon, Aug. 2015, South-Korea.

Elias Tsigaridas was invited speaker at

Workshop on Algebra, Geometry and Proofs in Symbolic Computation Thematic Program on Computer Algebra, Fields Inst. Toronto, Dec. 2015.

Structured Matrices Days 2015 June 4–5, 2015 XLIM-DMI, Université de Limoges, France.

Computer Algebra in Scientific Computing (CASC) September 14–18, 2015 RWTH Aachen University, Aachen, Germany.

9.1.5. Scientific expertise

Guénaél Renault had the following scientific expertise activities :

member of jury de selection du concours CR2 Inria Saclay

participating to the panel for research proposals selection in the field of theoretical computer science, Finland Academy.

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, 52 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

Licence : Numerical Algorithmic, 6 hours, L3, Université Pierre-et-Marie-Curie, France

Licence : Representations and Numerical Methods, 40 hours, L2, Université Pierre-et-Marie-Curie, France

Licence : Projects supervision, 20 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, 18 hours, M1, Université Pierre-et-Marie-Curie, France

Master : In charge of Introduction to polynomial systems 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

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

Mohab Safey El Din gave also a course at the “Ecole Jeunes Chercheurs 2015” of GDR IM.

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 : Simone Naldi, Exact algorithms for determinantal varieties and semidefinite programming, Univ. Toulouse, defended in Sept. 2015, Didier Henrion and Mohab Safey El Din

PhD in progress : Adrian Thillard, Countermeasures to side-channel attacks and secure multi-party computation, Damien Vergnaud, Emmanuel Prouff

PhD : Frédéric Urvoy de Portzamparc, Algebraic and physical security based on error-correcting codes, Université Pierre-et-Marie-Curie, defended in Apr. 2015, Jean-Charles Faugère and Ludovic Perret

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

PhD : Rina Zeitoun, Algebraic methods for the analysis of the security of cryptographic algorithms implementations, Université Pierre-et-Marie-Curie, defended in July 2015, Jean-Charles Faugère and Guénaël Renault

9.2.3. Juries

Jean-Charles Faugère was:

- reviewer and member of the PhD committee of Tristan Vaccon;
- member of the PhD committee of Simone Naldi;
- member of the PhD committee of Frédéric de Portzamparc;
- member of the PhD committee of Simone Naldi;

Ludovic Perret was:

- member of the PhD committee of Frédéric de Portzamparc;

Emmanuel Prouff was:

- member of the PhD committee of Luke Maher;
- member of the PhD committee of Mathieu Carbone;
- member of the PhD committee of Praveen Vадnala;
- member of the PhD committee of Sonia Belaid;
- member of the PhD committee of Sylvain Ruhault;
- member of the PhD committee of Vincent Grosso;
- member of the PhD committee of Annelie Heuser as reviewer;
- member of the PhD committee of Kevin Layat.

Guénaél Renault was:

- member of the PhD committee of Rina Zeitoun;
- member of mid-term evaluation committee of Nicolas Bruneau;

Mohab Safey El Din was:

- member of the PhD committee of Simone Naldi;
- member of the PhD committee of Frédéric Urvoy de Portzamparc;

Elias Tsigaridas was

- member of the PhD committee of Aaron Herman;
- member of the mid-term evaluation committee of Mario Cornejo-Ramirez;

9.3. Popularization

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

SECRET Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- WCC 2015 (Paris, April 13-17, 2015) has been organized by the project-team. The organizing committee is composed of A. Canteaut, G. Leurent, M. Naya Plasencia.
- N. Sendrier, co-organizer of Dagstuhl Seminar 15371, "Quantum Cryptanalysis", September 7-11, 2015, Dagstuhl, Germany.

9.1.1.2. Member of the organizing committees

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

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

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

9.1.2.2. Member of the conference program committees

- FSE 2015: March 8-11, 2015, Istanbul, Turkey (A. Canteaut, G. Leurent, M. Naya-Plasencia);
- CT-RSA 2015: April 20-24, 2015, San Francisco, USA (M. Naya-Plasencia);
- Eurocrypt 2015: April 26-30, 2015, Sofia, Bulgaria (A. Canteaut);
- Codes, Cryptology, and Information Security - C2SI 2015: May 26-28, 2015, Rabat, Morocco (A. Canteaut).
- Finite Fields and their applications $F_{q^{12}}$, Saratoga, USA, July 13-17, 2015 (A. Canteaut);
- SAC 2015: August 12-14, 2015, Sackville, Canada (M. Naya-Plasencia);
- Crypto 2015: August 16-20, 2015, Santa Barbara, USA (A. Canteaut);
- National workshop on Coding and Cryptography (Journées C2), October 5-9, 2015, La-Londe-Les-Maures, France (M. Naya-Plasencia, JP. Tillich);
- QCrypt 2015, Fifth annual conference on Quantum Cryptography, 28 September - 2 October 2015, Tokyo, Japan (A. Leverrier);
- ICCS 2015, International Conference on Coding and Cryptography, Alger, Algeria, November 2-5, 2015 (P. Charpin)
- Indocrypt 2015: December 6-9, 2015, Bangalore, India (A. Canteaut, G. Leurent)
- IMA-CC 2015, December 15-17, 2015, Oxford, UK (P. Charpin)
- 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 (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)

9.1.3. Journal

9.1.3.1. 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.

9.1.3.2. Guest editor for books or special issues

- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2015, co-editors: P. Charpin, N. Sendrier and J-P. Tillich.
- *Contemporary Developments in Finite Fields and Applications*, 2016, World Scientific Publishing, co-editor: A. Canteaut.

9.1.4. Invited talks

- A. Canteaut, *Differential Attacks Against SPN: A Thorough Analysis*, Codes, Cryptology, and Information Security - C2SI 2015, Rabat, Morocco, May 2015.
- G. Leurent, *Generic Attacks against MAC Algorithms*, Selected Areas in Cryptography - SAC 2015, Sackville, Canada, August 2013
- A. Leverrier, *Introduction to Quantum Cryptography*, WIC Symposium on Information Theory in the Benelux Brussels, Belgium, May 2015.
- J.P. Tillich *A survey on decoding quantum LDPC codes*, Quantum Information Processing - QIP 2015, Sydney, Australia, January 2015.

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

- A. Canteaut, *On the behaviors of affine equivalent Sboxes regarding differential and linear attacks*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- A. Canteaut, *Sur la résistance aux cryptanalyses différentielles et linéaires*, Journées Codage et Cryptographie 2015, La Londe-les-Maures, France, October 2015.
- A. Chailloux *Arbitrarily long relativistic bit commitment*, QuPa - Quantum Information in Paris, Paris, France, December 2015.
- A. Chailloux *Introduction to Quantum Cryptography*, 9ème Journées Scientifiques de l'Université de Toulon - France, April 2015.
- A. Chailloux *Introduction à l'Informatique Quantique*, ENS Lyon Seminar, France, January 2015.
- G. Leurent, *On cryptanalysis of the Chaskey MAC*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- G. Leurent, *Generic Attacks against MAC Algorithms*, Asian Workshop on Symmetric Key Cryptography - ASK 2015, Singapore, September 201
- A. Leverrier, *Quantum differential cryptanalysis*, Dagstuhl Seminar Quantum Cryptanalysis, Dagstuhl, Germany, 7-11 September 2015.
- A. Leverrier, *Quantum expander codes*, QuPa - Quantum information in Paris, France, 7-8 December 2015.
- M. Naya-Plasencia, *On impossible differential attacks*, Early Symmetric Crypto - ESC 2015, Clervaux, Luxemburg, January 2015.
- N. Sendrier, *Best known attacks on code-based cryptosystems: state of the art and perspectives*, DIMACS Workshop on the Mathematics of Post-Quantum Cryptography, Piscataway, USA, January 2015.

9.1.5. 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>;
- Since Autumn 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.

9.1.6. Research administration

- N. Sendrier is a vice-chair of the “Commission d’Evaluation” at Inria;
- A. Canteaut is a member of the “Comité de pilotage” of the Fondation Sciences Mathématiques de Paris;
- N. Sendrier is a member of the committee PEDR INS2I (CNRS) 2015
- N. Sendrier is a member of the committee for PhD fundings, EDITE, Commission thématique O (RO, Algo, Calcul et Programmation).
- J.-P. Tillich is in charge of “Formation par la recherche” for the Paris-Rocquencourt Inria center.
- **Committees for the selection of professors, assistant professors and researchers:** Inria Directeurs de recherche (N. Sendrier), Inria Paris-Rocquencourt Chargés de recherche (A. Canteaut), Université Rennes 1 MC (M. Naya Plasencia), Université de Limoges PR (A. Canteaut)
- Inria Jury d’admission, Directeurs de recherche and Chargés de recherche (N. Sendrier)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

Master: A. Canteaut, *Error-correcting codes and applications to cryptology*, 11 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: 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:

- *IACR School on Design and security of cryptographic algorithms and devices*, Sardinia, Italy, Oct. 18-23, 2015: A. Canteaut.

A. Canteaut, M. Naya-Plasencia and JP. Tillich gave several lectures on symmetric cryptography at Thales.

9.2.2. Supervision

PhD: Joëlle Roué, *Analysis of the resistance of block ciphers against linear and differential attacks*, University Pierre-et-Marie Curie, October 14, 2015, supervisor: A. Canteaut

PhD: Audrey Tixier, *Blind identification of error-correcting codes*, University Pierre-et-Marie Curie, October 14, 2015, supervisor: J.P. Tillich

PhD in progress: Virginie Lallemand, *Cryptanalysis for symmetric cryptography*, since October 2013, 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, , 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

9.2.3. Juries

- Martin M. Lauridsen, *Design and Analysis of Symmetric primitives*, Technical University of Denmark (DTU), October 26, 2015, committee: A. Canteaut (reviewer).
- Carl Löndahl, *Some Notes on Code-Based Cryptography*, Lund University, February 6, 2015, committee: N. Sendrier (opponent)
- Joëlle Roué, *Analysis of the resistance of block ciphers against linear and differential attacks*, University Pierre-et-Marie Curie, October 14, 2015, committee: A. Canteaut (supervisor), M. Naya Plasencia.
- Sylvain Ruhault, *Security Analysis for Pseudo-Random Number Generators*, École Normale Supérieure, June 30, 2015, committee: N. Sendrier
- Audrey Tixier, *Blind identification of error-correcting codes*, University Pierre-et-Marie Curie, October 14, 2015, committee: J.P. Tillich (supervisor), N. Sendrier
- Gaël Thomas, *Design and security analysis for constructions in symmetric cryptography*, University of Limoges, May 13, 2015, committee: A. Canteaut (chair).

9.3. Popularization

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

SPECFUN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- A. Bostan has served in the organizing committee of the *Journées Nationales de Calcul Formel* (JNCF 2015), the annual meeting of the French computer algebra community.
- A. Mahboubi has served in the organizing and scientific committees of *Mathematics, Algorithms and Proofs* (MAP 2016).

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

- A. Bostan is part of the Scientific advisory board of the conference series *Conference on Effective Methods in Algebraic Geometry* (MEGA).
- F. Chyzak has served as a conference program committee member for the *Conference on Intelligent Computer Mathematics* (CICM 2015).
- A. Mahboubi has served as a program committee member for the *25th International Conference on Automated Deduction* (CADE 25).
- A. Mahboubi has served as a program committee member for the *21st International Conference on Types for Proofs and Programs* (TYPES 2015).
- A. Mahboubi has served as a program committee member for the *Workshop on Logical Frameworks and Meta-Languages: Theory and Practice* (LFMTP 2015).

9.1.2.2. Reviewer

- A. Bostan has served as reviewer for the *International Symposium on Symbolic and Algebraic Computation* (ISSAC 2015).
- F. Chyzak has served as reviewer for the *International Symposium on Symbolic and Algebraic Computation* (ISSAC 2015).
- A. Mahboubi has served as reviewer for the international conferences *NASA Formal Methods Symposium* (NFM 2015), *Certified Programs and Proofs* (CPP 2015), *Typed Lambda Calculi and Applications* (TLCA 2015), *Conference on Intelligent Computer Mathematics* (CICM 2015) and for the national conference *Journées Nationales des Langages Applicatifs* (JFLA 2015).
- Th. Sibut-Pinote has served as reviewer for the *International Conference on Automated Deduction* (CADE 2015).

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

- A. Bostan has served as reviewer for the *Journal of Symbolic Computation*, the *Journal of Complexity and Applicable Algebra in Engineering, Communication and Computing*.
- F. Chyzak has served several times as a reviewer for the *Journal of Symbolic Computation*.
- A. Mahboubi has served as a reviewer for the *Journal of Formalized Reasoning* and several times for *Journal of Automated Reasoning*.

9.1.4. Invited talks

- A. Bostan has given an invited 3-hours lecture at the Séminaire Lotharingien de Combinatoire in Ellwangen, Germany (March 2015) and another 3-hours lecture at the *SFB-Workshop on Restricted Lattice Walks* in RISC, Hagenberg, Austria (May 2015).
- A. Bostan has given an invited talk in the conference *Automatic Sequences, Number Theory, and Aperiodic Order*, held at the Technical University of Delft, Netherlands (Oct 2015).
- A. Bostan has given a talk during the *Thematic Program on Computer Algebra* (Fields Institute, Toronto, Canada, September 2015).
- F. Chyzak has given a number of talks on his ongoing work (joint with A. Bostan of the team) on obtaining hypergeometric closed-form expressions in the enumerative combinatorics of walks: *Functional Equations in Limoges* (Limoges, March 2015), *Thematic Program on Computer Algebra* (Fields Institute, Toronto, Canada, September 2015), *Séminaire Philippe Flajolet* (Institut Henri Poincaré, Paris, October 2015).
- A. Mahboubi has given an invited talk common to the conferences *14th Asian Logic Conference* (ALC 15) and *6th Indian Conference on Logic and its Application* (ICLA 15), in Mumbai, India (January 2015).
- A. Mahboubi has given an invited talk to the Workshop on Homotopy Type Theory / Univalent Foundations, satellite of the International Conference on Rewriting, Deduction, and Programming, in Warsaw, Poland (July 2015).
- A. Mahboubi has given a talk during the *Thematic Program on Computer Algebra* (Fields Institute, Toronto, Canada, December 2015).

9.1.5. Scientific expertise

- F. Chyzak is member of the steering committee of the *Journées Nationales de Calcul Formel* (JNCF 2015), the annual meeting of the French computer algebra community.
- A. Mahboubi has been nominated as a member of the management committee the COST action EUTYPES (CA15123) *The European research network on types for programming and verification*, coordinated by Herman Geuvers.

9.1.6. Research administration

- A. Mahboubi is a member of the *Commission Scientifique* of the Inria–Saclay–Île-de-France center.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: A. Bostan, *Algorithmes efficaces en calcul formel*, 18h, M2, MPRI, France

Master: F. Chyzak, *Algorithmes efficaces en calcul formel*, 4.5h, M2, MPRI, France

Master: A. Mahboubi, *Assistants de preuve*, 18h, M2, MPRI, France

License: L. Dumont, various courses, 64h, Université Paris-Sud, France.

License: Th. Sibut-Pinote, various courses, 64h, École Polytechnique, France.

9.2.2. Supervision

- PhD in progress: L. Dumont, *Algorithmique efficace pour les diagonales, applications en combinatoire, physique et théorie des nombres*, École Polytechnique, started in September 2013, supervised by A. Bostan and B. Salvy.
- PhD in progress: Th. Sibut-Pinote, *Calcul numérique et démonstrations mathématiques, de la rigueur à la preuve formelle*, École Polytechnique, started in September 2014, supervised by A. Mahboubi.

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

9.2.3. Juries

- A. Bostan has served as a jury member of the French *Agrégation de Mathématiques – épreuve de modélisation, option C*.
- A. Bostan has served as an examiner in the PhD jury of Cuang Tran, *Calcul formel dans la base des polynômes unitaires de Chebyshev*, Université Paris 6, October 9, 2015.
- F. Chyzak has served as an examiner in the PhD jury of Suzy Maddah, *Formal Reduction of Differential Systems*, Université de Limoges, September 25, 2015.
- A. Mahboubi has served as an examiner in the half-way PhD defense of Pierre Boutry, *Learning environment for interactive proof in geometry*, University of Strasbourg, June 15th, 2015.

9.3. Popularization

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

VEGAS Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing committees

Sylvain Lazard organized with S. Whitesides (Victoria University) the 14th Inria - McGill - Victoria Workshop on Computational Geometry⁰ at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

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

Monique Teillaud co-organized the Dagstuhl Seminar on Computational Geometry, with Otfried Cheong (KAIST, Korea) and Jeff Erickson (University of Illinois at Urbana-Champaign), Leibniz-Zentrum für Informatik, Germany, March 9-13. <http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=15111>

Monique Teillaud co-organized the Workshop on Computational Geometry in non-Euclidean Spaces, with Éric Colin de Verdière (CNRS, ENS Paris) and Jean-Marc Schlenker (Mathematics Research Unit, U. Luxembourg), Inria, Loria, Nancy, August 26-28. The slides of the talks are available on the workshop website <http://neg15.loria.fr/>.

Monique Teillaud and Marc Pouget organized the 39th **CGAL** Developer Meeting, Sept 28 - Oct 2 at Inria Nancy - Grand Est.

8.1.2. Scientific events selection

8.1.2.1. Member of the conference program committees

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

8.1.2.2. 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.

8.1.3. Journal

8.1.3.1. Member of the editorial boards

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

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

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

8.1.3.2. 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.

⁰Workshop on Computational Geometry

8.1.4. Invited talks

Guillaume Moroz was invited to give a talk at the Fields Institute in Toronto for the workshop on Algebra, Geometry and Proofs in Symbolic Computation. He was also invited to give a talk at the IHP for the seminar on algorithmic and computational geometry and at Supelec.

8.1.5. Research administration

8.1.5.1. Hiring committees

S. Lazard was president of the hiring committee for a Professor position (UL/ENSEM/LORIA).

8.1.5.2. Steering Committees

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

8.1.5.3. 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.

8.1.5.4. Local committees and responsibilities

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).

M. Teillaud is a member of the CDT, *Commission de développement technologique*, of Inria Nancy - Grand Est.

8.1.5.5. 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 Symposium on Computational Geometry.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Guillaume Moroz, *Géométrie algébrique et applications en robotique*, 12h, M1, École Mathématique Africaine, Sénégal.⁰

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

Licence: Laurent Dupont, *Algorithmique*, 72h, 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.

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

⁰<http://nlaga-simons.ucad.sn/index.php/new-international-events>

8.2.2. Supervision

PhD: Rémy Thomasse, Complexity analysis of random convex hulls, defended December 18th 2015. The student is hosted in EPI GEOMETRICA but supervised by O. Devillers [10].

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

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

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

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

8.2.3. Juries

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

S. Lazard was an external examiner (rapporteur) of the Ph.D. of Cuong Tran (Univ. Pierre et Marie Curie).

8.3. Popularization

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

ALF Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

- André Seznec is the PC chair for ISCA 2016.
- Isabelle Puaut and Damien Hardy have organized the Ecole d'été Temps Réel in Rennes in August 2015.
- Isabelle Puaut is the chair of the RTNS steering committee.

10.1.1.2. Member of the organizing committees

- Isabelle Puaut is a member of the Executive committee of IEEE Technical Committee on Real-Time Systems
- Isabelle Puaut is member of the Steering committees of ECRTS and WCET conferences.
- Sylvain Collange was a member of the organization committee of Rencontres Arithmétiques de l'Informatique Mathématique (RAIM) 2015 in Rennes.

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

- André Seznec is the PC chair for ISCA 2016.

10.1.2.2. Member of the conference program committees

- Isabelle Puaut was a member of ECRTS 2015, RTAS 2015, RTCSA 2015 RTNS 2015 and WCET 2015 program committees. She is a member of the ECRTS 2016 program committee.
- Damien Hardy was a member of RTNS 2015 and WCET 2015 program committees
- André Seznec was a member of the MICRO 2015 and the SAMOS 2015 program committees.
- Pierre Michaud was a member of the program committee of the OMHI 2015 workshop.
- Erven Rohou was a member of the program committee of DITAM-PARMA and ISPA 2015.
- Sylvain Collange is a member of the ISCA 2016 program committee.

10.1.2.3. Reviewer

ALF members have been reviewers for many conferences and journals.

10.1.3. Journal

10.1.3.1. Member of the editorial boards

- André Seznec is a member of the editorial board of IEEE Micro and an associate editor of ACM TACO.

10.1.3.2. Reviewer - Reviewing activities

ALF members have been reviewers for many conferences and journals.

10.1.4. Invited talks

- Isabelle Puaut. "Multicore timing verification: towards more integrated WCET and schedulability analysis. TACLe COST action Focussed meeting on timing analysis of parallel programs in many-core architectures". Porto, Portugal, Nov. 2015.
- André Seznec. "Skewed Compressed Cache", AMD, Sunnyvale, Aug. 2015
- Arthur Perais. "Cost-Effective Speculative Scheduling in High Performance Processors" Intel, Hillsboro June 2015
- Damien Hardy . "Worst Case Execution Time Estimation and Permanent Faults" at "9ièmes rencontres de la communauté française de compilation", Jan. 2015.
- Erven Rohou. "Branch Prediction and the Performance of Interpreters: Don't Trust Folklore", at Dixièmes rencontres de la communauté française de compilation, Sep 2015.
- Erven Rohou. "Traceability of Flow Information: Reconciling Compiler Optimizations and WCET Estimation", at Neuvièmes rencontres de la communauté française de compilation, Jan 2015.

10.1.5. Scientific expertise

André Seznec was member of the ERC Advanced grants panel.

10.1.6. Research administration

- Erven Rohou is a member of the Inria CDT (Commission du Développement Technologique)
- As "correspondant scientifique des relations internationales" for Inria Rennes Bretagne Atlantique, Erven Rohou is a member of the Inria COST GTRI (Groupe de Travail "Relations Internationales" du Comité d'Orientation Scientifique et Technologique).
- A. Seznec is an elected member of the administration board of Inria since November 2014.
- Erven Rohou was a member of the Inria CR2 recruitment committee.
- Erven Rohou was a member of the recruitment committee of an assistant professor at Uppsala University (Sweden).
- Isabelle Puaut is member of the ISTIC council.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master research : A. Seznec, E.Rohou, I. Puaut, Performance et Microarchitecture, 24 hours, M2, Université de Rennes I, France

Master research: I. Puaut, E. Rohou, Rédaction d'articles scientifiques, 18 hours, M2, Université de Rennes I, France

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

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

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

Master: D. Hardy Systèmes d'exploitation, 40 hours, M1, Université de Rennes I, France

Master: D. Hardy Systèmes d'exploitation, 60 hours, M2 CCI, Université de Rennes I, France

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

Master/PhD: S. Collange, GPU programming, 30 hours, MSc/PhD programs, Universidade Federal de Minas Gerais, Brazil

10.2.2. Supervision

HdR: Erven Rohou, Infrastructures and Compilation Strategies for the Performance of Computing Systems, Université Rennes 1, Nov 2015

PhD : Hanbing Li, Extraction and Traceability of Annotations for WCET Estimation, Université Rennes 1, Oct 2015, co-advisors E. Rohou and I. Puaut

PhD : Arthur Perais, "Increasing the performance of superscalar processors through value prediction", Université Rennes 1, Sept 2015, advisor A. Seznec

PhD : Surya Khizakanchery Natarajan, "Modeling performance of serial and parallel sections of multi-threaded programs in manycore era", Université Rennes 1, June 2016, advisor A. Seznec

PhD : Bharath Narasimha Swamy, "Exploiting heterogeneous manycores on sequential code", Université Rennes 1, March 2015, advisor A. Seznec

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

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

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

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

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

PhD in progress : Rabab Bouziane, Université Rennes 1, Nov 2015, advisor E. Rohou

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: Benjamin Rouxel, Université Rennes 1, Oct 2015, co-advisors I. Puaut and S. Derrien

PhD in progress: Viet Anh Nguyen, Université Rennes 1, Jan 2015, co-advisors D. Hardy and I. Puaut

10.2.3. Juries

The member of ALF have participated to many PhD defense juries in France and abroad.

ATEAMS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- Tijs van der Storm: co-organizer of the 3rd Workshop on Domain-Specific Language Design and Implementation (DSLDFI'15).

9.1.1.2. Member of the organizing committees

- Tijs van der Storm: Publicity co-chair SPLASH and track organizer SPLASH-I
- Jurgen Vinju: co-organizer Bits & Chips Software Event (Legacy Software Track), Eindhoven, The Netherlands

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

- Paul Klint: International Conference on Software Language Engineering (SLE'15), 14th edition of the BELgian-NEtherlands software eVOLution seminar (BENEVOL 2015), 22nd IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER'15)
- Tijs van der Storm: International Conference on Model Transformation (ICMT'15), International Conference on Software Language Engineering (SLE'15), Transformation Tool Context (TTC'15), Future Programming Workshop (FPW'15).
- Jurgen Vinju: 10th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE'15), 3rd International Workshop on The Globalization of Modeling Languages Workshop (GEMOC'15), 5th Summer School on Grand Timely Topics in Software Engineering (GTTSE'15), IEEE International Conference on Software Comprehension (ICPC'15), 14th edition of the BELgian-NEtherlands software eVOLution seminar (BENEVOL 2015).

9.1.2.2. Reviewer

9.1.2.2.1. Journal

- Member of the editorial boards:
 - Paul Klint: editor of Science of Computer Programming (Elsevier SCP)
- Reviewer - Reviewing activities:
 - Paul Klint: Science of Computer Programming
 - Tijs van der Storm: Science of Computer Programming (SCP), Computer Languages and Systems (COMLAN)
 - Jurgen Vinju: Science of Computer Programming (SCP), Computer Languages and Systems (COMLAN), Journal on Empirical Software Engineering (ESE), Journal of Software Maintenance and Evolution (JSME)

9.1.3. Invited talks

- Textual and projectional language workbenches. Tijs van der Storm, Dagstuhl on “Domain-Specific Languages”.
- “Software Engineering: The War Against Complexity”, Jurgen Vinju. CHA-Q Open Tool Demonstrations Event (keynote), February 24, Antwerpen, Belgium.

- “Program Analysis and Transformation with Rascal” tutorial at the 36th annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI) in Portland, USA. Mark Hills, Jurgen Vinju, Paul Klint.

9.1.4. Leadership within the scientific community

9.1.4.1. Member of steering committees

- Jurgen Vinju: International Conference on Software Language Engineering (ACM SLE) (*chair*)
- Jurgen Vinju: International Working Conference on Source Analysis and Manipulation (IEEE SCAM)

9.1.4.2. Member of other groups

- Jurgen Vinju: Member of IFIP WG 2.3 — Working Group on Software Implementation Technology
- Tijs van der Storm: Member of IFIP WG 2.16 — Working Group on Language Design
- Tijs van der Storm: Member of the board of European Association for Programming Languages and Systems (EAPLS)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Tijs van der Storm, “Software Construction”, Masters, Universiteit van Amsterdam

Jurgen J. Vinju, “Software Evolution”, Masters, Universiteit van Amsterdam

9.2.2. Supervision

PhD : Atze van der Ploeg, “Efficient Abstractions for Visualization and Interaction”, Universiteit van Amsterdam, April, 8th, 2015 [48] (advisors: Tijs van der Storm and Paul Klint)

PhD in progress : Ali Afroozeh, “Closing the Book on Parsing”, 2017 (advisors: Jurgen Vinju and Paul Klint)

PhD in progress : Pablo Inostroza Valdera, “Modular Language Implementation with Object Algebras”, 2018 (advisors: Tijs van der Storm and Paul Klint)

PhD in progress : Anastasia Izmaylova, “Parser Combinators Revisited”, 2017 (advisors: Jurgen Vinju and Paul Klint)

PhD in progress : Davy Landman, “Source Code Complexity in Context”, 2016 (advisors: Jurgen Vinju and Paul Klint)

PhD in progress : Riemer van Rozen, “Domain-Specific Languages for Game Development”, 2017 (advisors: Paul Klint and Tijs van der Storm)

PhD in progress : Michael Steindorfer, “Fast and Lean Immutable Data Structures”, 2017 (advisors: Jurgen Vinju and Paul Klint)

PhD in progress : Jouke Stoel, “Solving the Bank”, 2019 (advisors: Jurgen Vinju and Tijs van der Storm)

Msc : Zisimopolous, P.: “A Grid Scheduling infrastructure for SmartConnect’s performance monitoring calculations”, Universiteit van Amsterdam, The Netherlands

Msc : Zhelyazkov, A.T.: “Form controls in WebGL. A stepping stone to a WebGL library for developing commercial interactive 3D websites”, Universiteit van Amsterdam, The Netherlands

Msc : Valencia Vargas, S.: “Begelman vs. FolkRank. The Comparison of Two Algorithms in the Tag Recommendation Context: An Exploratory Study”, Universiteit van Amsterdam, The Netherlands

Msc : Heimensen, M.: “JavaScript language extension with language workbenches”, Universiteit van Amsterdam, The Netherlands

Msc : Harezlak, H.: “Geographically-aware scaling for real-time persistent WebSocket applications”, Universiteit van Amsterdam, The Netherlands

Msc: Chow, K.: “Performance of Face Recognition Algorithms on Mobile Devices”, Universiteit van Amsterdam, The Netherlands

Msc: Iwan Flaming: “An automatic CSRF protection tool”, Universiteit van Amsterdam, The Netherlands

Msc: Omar Pakker: “Graph-Based Querying On top of the Entity Framework”, Universiteit van Amsterdam, The Netherlands

9.2.3. *Juries*

- Jurgen Vinju:
 - Phd Reza Yazdanshenas, A. — Universitet i Oslo, Norway
 - Phd Hafeez Osman, M. — Universiteit Leiden, The Netherlands

9.3. Popularization

- Ali Afroozeh and Anastasia Izmaylova: “Meerkat parsers: a general parser combinator library for real programming languages”, Scala Days 2015, Amsterdam, The Netherlands.
- Paul Klint: “Paul Klint in RTL Nieuws over het nieuwe betalingssysteem van het pgb” (radio interview).
- Paul Klint: “De evolutie van codetaal”, media appearance, NRC Handelsblad
- Paul Klint: “Première internetfilm over Nederlands informatica erfgoed”, media appearance, Automatisering Gids.
- Paul Klint: “Remembering Arra: a pioneer in Dutch computing”, media appearance, <http://www.engineersonline.nl/>.
- Davy Landman: “Let’s talk about complexity”, Devnology software development community talk, Amsterdam, The Netherlands.
- Tijs van der Storm: “Opportunities and Risks of MDSE: experience with Derric, a DSL for Digital Forensics”, Bits&Chips industry conference.
- Jouke Stoel and Tijs van der Storm: “Hack Your Language with Rascal”, workshop at Joy of Coding conference, Rotterdam, The Netherlands.
- Tijs van der Storm, “Live Little Languages”, JBI Colloquium, Groningen, The Netherlands.
- Jurgen Vinju: “Public/Private Collaboration {in,for,with} Software Engineering”, 21st Annual Conference of the European Association of Research Managers and Administrators, Leiden, The Netherlands
- Jurgen Vinju: OSSMETER Pitch EU Concertation Meeting - Turning cloud research into innovative software & services, March 25th 2015, Brussels, Belgium.
- Jurgen Vinju: Challenges and Opportunities of Big Software-based Innovation NWO Big Software Match Making Day, July 1st, 2015, Utrecht, The Netherlands.

CAIRN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events selection

9.1.1.1. Chair of conference program committees

A. Tisserand was program co-chair of the 22nd IEEE Symposium on Computer Arithmetic (Lyon, 22-24 June 2015) [65].

O. Sentieys was Track Chair at IEEE NEWCAS.

9.1.1.2. 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.

A. Tisserand was a member of technical program committee of the following conferences: IEEE ARITH 2015, DASIP 2015, IEEE NEWCAS 2015, IEEE PATMOS 2015 and IEEE Reconfig 2015.

S. Derrien was a member of technical program committee of IEEE FPL.

O. Sentieys was a member of technical program committee of IEEE FPL, ACM ENSSys, FSP, FPGA4GPC.

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, Advances in Computer Engineering, and International Journal of Distributed Sensor Networks.

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

9.1.3. Invited talks

O. Sentieys gave an invited lecture at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Louvain, Belgium, in January 2015 on "Domain-Specific Computing Platforms: the Ultimate Energy-Efficiency of Hardware Accelerators".

O. Sentieys gave an invited lecture at The 1st International Workshop on Optical/Photonic Interconnects for Computing Systems (OPTICS Workshop), co-located with IEEE/ACM Design Automation and Test in Europe (DATE'15), in March 2015 on "Bandwidth Requirements in Manycore Architectures: What Can 3D Bring?".

A. Tisserand has been invited speaker at the international conference on elliptic curve cryptography (ECC) [29].

A. Tisserand gave an invited lecture at the CNRS ARCHI 2015 summer school on "Processor Extensions for Security".

9.1.4. Leadership within the scientific community

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

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

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

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

D. Chillet was member of the French National University Council since 2009 in signal processing and electronics (Conseil National des Universités en 61e section).

D. Chillet was member of the Permanent Committee of the French National University Council since November 2011 in signal processing and electronics (Commission Permanente du Conseil National des Universités en 61e section).

A. Tisserand was member of the French National University Council since 2011 in computer science (Conseil National des Universités en 27e section).

O. Sentieys was responsible for some scientific evaluations (HCERES).

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, University of Science and Technology 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 University of Science and Technology of Hanoi (M1)
- D. Chillet: embedded processor architecture, 20h, ENSSAT (M1)
- D. Chillet: VHDL, 10h, ENSSAT (M1)
- D. Chillet: multimedia processor architectures, 24h, ENSSAT (M2)
- D. Chillet: advanced processor architectures, 24h, Master by Research (SISEA) and ENSSAT (M2)
- D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne and University of Occidental Brittany (UBO) (M2)
- 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)
- A. Kritikakou: computer architecture, 50h, ISTIC, Univ. Rennes 1 (L3)

- A. Kritikakou: operating systems, 24h, 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)
- A. Tisserand: multiprocessor architectures and programming, 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.
- P. Quinton was the director of Ecole Normale Supérieure de Rennes until end Aug. 2015.
- D. Chillet was the Director of Academic Studies of ENSSAT until end Aug. 2015.
- S. Derrien is the responsible of the first year of the Master of Computer Science at ISTIC since Sep. 2012.
- O. Sentieys is responsible of the "Embedded Systems" branch of the SISEA Master by Research.
- D. Chillet is the responsible of the ICT Master of University of Science and Technology of Hanoi and also co-responsible of the "Embedded Systems" speciality of this master.
- 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: Christophe Huriaux, Embedded reconfigurable hardware accelerators with efficient dynamic reconfiguration management, Dec. 2015, O. Sentieys, A. Courta.
- PhD: Quang-Hai Khuat, Real-Time Spatio-Temporal Task Scheduling on 3D Architectures, Feb. 2015, D. Chillet.
- PhD in progress: Benjamin Barrois, Approximate Computing: a New Paradigm for Energy-Efficient Computing Architectures, Oct. 2014, O. Sentieys.
- PhD in progress: Florent Berthier, Study and Design of an Ultra Low Power Asynchronous Core for Sensor Networks, Oct. 2013, O. Sentieys, P. Vivet, E. Beigne.
- PhD in progress: Franck Bucheron, Secure Virtualization for Embedded Systems, Oct. 2011, A. Tisserand.
- PhD in progress: Gaël Deest, Computing with Errors: Error-Tolerant Machine Code Generation for Unreliable Embedded Hardware, Oct. 2013, S. Derrien, O. Sentieys.
- PhD in progress: Ali Hassan El-Moussawi, Performance/Accuracy Trade-Off in Automatic Parallelization for Embedded Many-Core Platforms, Nov. 2012, S. Derrien.
- PhD in progress: Gabriel Gallin, Hardware Arithmetic Units and Crypto-Processor for Hyperelliptic Curves Cryptography, Oct. 2014, A. Tisserand, N. Veyrat-Charvillon.
- PhD in progress: 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, Dec. 2015, 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: Jérémie Métairie, Reconfigurable Arithmetic Units for Secure Cryptoprocessors, Oct. 2012, A. Tisserand, E. Casseau.

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: 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 organisation

10.1.1.1. Member of the organizing committees

Cédric Bastoul has been co-organizing the HIP3ES 2015 workshop (High Performance Energy Efficient Embedded Systems) held in conjunction with the international conference HiPEAC 2015. He is also currently organizing the next HIP3ES event, to be held in conjunction with the international conference HiPEAC 2016.

10.1.2. Scientific events selection

10.1.2.1. Member of the conference program committees

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

Philippe Clauss has been part of the program committee of the third workshop on Energy Efficient Super Computing (E2SC), held in conjunction with SC15.

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

Cédric Bastoul and Vincent Loechner have been part of the program committee of both HIP3ES 2015 and HIP3ES 2016 (International Workshop on High Performance Energy Efficient Embedded Systems), held in conjunction with the international conferences HiPEAC 2015 (resp. HiPEAC 2016).

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

Cédric Bastoul has been part of the program committee of PARMA+DITAM 2015 and PARMA+DITAM 2016 (Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures + Workshop on Design Tools and Architectures for Multicore Embedded Computing Platforms), held in conjunction with HiPEAC 2015 (resp. HiPEAC 2016).

10.1.2.2. Reviewer

Cédric Bastoul has been reviewer for the following conferences and workshops: PARMA 2015 and 2016 (International Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures), IMPACT 2016 (International Workshop on Polyhedral Compilation Techniques), HIP3ES 2015 and 2016 (International Workshop on High Performance Energy Efficient Embedded Systems).

10.1.3. Journal

10.1.3.1. Editorial board membership

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

In 2014, the [episcience](#) platform for open access journals has been created in a joint effort by Inria and CNRS. In 2015, DMTCS, as one of the first journals, has moved to this platform presenting a new [server interface](#) which lives on top of the national scientific archive [HAL](#). We have been a driving force in the definition and debugging of the new platform, see [1].

10.1.3.2. Reviewer - Reviewing activities

Jens Gustedt has served as a reviewer for *Theory of Computing Systems* and *IEEE Transactions on Parallel and Distributed Systems*.

Philippe Clauss has served as a reviewer for the following journals: *ACM Transactions on Architecture and Code Optimization*, *ACM Transactions on Programming Languages and Systems*.

Alain Ketterlin has served as a reviewer for the following journals: *Parallel Computing*, and *International Journal of Parallel Programming*. He has also served as sub-reviewer for the PACT 2015 conference.

Cédric Bastoul has been reviewer for the *Parallel Computing international journal* (ParCo).

10.1.4. Scientific expertise

Cédric Bastoul has been an expert for the European Commission for the call FETHPC of the H2020 programme. He also has been an expert for the French research ministry and the French finance ministry for the research tax credit programme.

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, see [27].

This work on the C programming language also gave rise to the proposal of a language extension, **Modular C**, see [25].

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence : Alain Ketterlin, Algorithmique et Structures de Données (Licence de Mathématique), 40h, L3, Université de Strasbourg, France

Licence : Alain Ketterlin, Réseaux et Protocoles (Licence d'Informatique), 64h, L3, Université de Strasbourg, France

Master : Alain Ketterlin, Ingénierie de la preuve, 21h, M1, Université de Strasbourg, France.

Licence : Alain Ketterlin, Architecture et Programmation des mécanismes de base d'un système informatique, 68h, L1 (IUT), Université de Strasbourg, France.

Licence : Alain Ketterlin, Modèles de calcul, 14h, L1, 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

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 : Vincent Loechner, Systèmes d'exploitation, 38h, 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 : Eric Violard, Programmation Fonctionnelle, 21h, L2, Université de Strasbourg, France
 Licence : Eric Violard, Architecture des Ordinateurs, 16h, L2, Université de Strasbourg, France
 Licence : Eric Violard, Logique et Programmation Logique, 26h, L2, Université de Strasbourg, France
 Licence : Eric Violard, Algorithmique et Structure de Données, 35h, L3, Université de Strasbourg, France
 Licence : Cédric Bastoul, Architecture, 68h, L1 (IUT), Strasbourg University, France
 Licence : Cédric Bastoul, Operating Systems, 16h, L2, Strasbourg University, France
 Licence : Cédric Bastoul, Concurrent Systems, 19h, L3, Strasbourg University, France
 Master : Cédric Bastoul, Compiler Design, 48h, M1, Strasbourg University, France
 Master : Cédric Bastoul, Advanced Compilation, 23h, M1, Strasbourg University, France
 Master : Cédric Bastoul, Parallelism, 16h, M1, Strasbourg University, France
 Master : Cédric Bastoul, Introduction to Research, 7h, L3+M1, Strasbourg University, France

10.2.2. Supervision

PhD in progress: Yann Barsamian, *Space-Filling Curves and their Application to the Numerical Resolution of Vlasov Equations*, since Oct 2014, Eric Violard

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

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

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

PhD in progress: Luis Esteban Campostrini, *Virtual linear data layout*, since January 2015, Philippe Clauss

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

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

PhD: Aravind Sukumaran-Rajam, *Beyond the Realm of the Polyhedral Model: Combining Speculative Program Parallelization with Polyhedral Compilation*, University of Strasbourg, November the 5th, 2015, Philippe Clauss

PhD: Imen Fassi, *XFOR (Multifor): A New Programming Structure to Ease the Formulation of Efficient Loop Optimizations*, University of Strasbourg, November the 27th, 2015, Philippe Clauss

PhD: Jean-François Dollinger, *A framework for efficient execution on GPU and CPU+GPU systems*, University of Strasbourg, July the 1st, 2015, Vincent Loechner and Philippe Clauss

10.2.3. Juries

Jens Gustedt participated to the following PhD jury in 2015:

Date	Candidate	Place	Role
July 8	Florian David	Univ. Pierre et Marie Curie, Paris	Examiner

Philippe Clauss participated to the following PhD juries in 2015:

Date	Candidate	Place	Role
Oct. 9	Hangbing Li	Univ. Rennes 1	Reviewer
Sept. 18	Nicolas Triquenaux	Univ. Versailles Saint-Quentin-en-Yvelines	Reviewer

Alain Ketterlin was a member of the following PhD juries in 2015:

Date	Candidate	Place	Role
Mar. 5	Bharath Narasimha-Swamy (Adv.: André Sez nec)	Univ. Rennes 1	Examiner
Nov. 5	Fabien Rozar (Adv.: Jean Roman & Guillaume Latu)	Univ. Bordeaux	Examiner

Cédric Bastoul participated to the following HDR jury in 2015:

Date	Candidate	Place	Role
May 18	Corinne Ancourt	École des Mines de Paris	President
Nov. 2	Erven Rohou	Université de Rennes 1	Examiner

Cédric Bastoul participated to the following PhD juries in 2015:

Date	Candidate	Place	Role
September 25	Riyadh Badhdadi	Pierre et Marie Curie University	Reviewer

10.3. Popularization

Jens Gustedt is regularly blogging about efficient programming, in particular about the **C programming language**. He also is an active member of the **stackoverflow community** a technical Q&A site for programming and related subjects. A book about **modern C** is in preparation.

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

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

COMPSYS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organization

10.1.1.1. General Chair, Scientific Chair

Laure Gonnord is co-chair of the “french compilation community”, with Florian Brandner (ENSTA, then Telecom ParisTech) and Fabrice Rastello (Inria Corse).

Alain Darté 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. Also, Alain Darté and Alexandre Isoard participated to CPC’15 in London (Jan. 15).

10.1.1.2. Member of Organizing Committees

Alain Darté was co-organizer of IMPACT’15 (International Workshop on Polyhedral Compilation Techniques) and Tomofumi Yuki is co-organizer of IMPACT’16.

Tomofumi Yuki was publicity co-chair of GPCE 2015 (15th International Conference on Generative Programming: Concepts & Experience).

Alain Darté and Tomofumi Yuki are currently organizing a second polyhedral spring school in 2016, with connections with HPC users from numerical analysis.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Alain Darté was program co-chair of IMPACT’15, with Alexandra Jimborean (Uppsala University). Tomofumi Yuki is program co-chair of IMPACT’16, with Michelle Strout (University of Arizona).

Alain Darté was program chair of the topic E2 “Compilers for Embedded Systems” of DATE’15 (International Conference on Design, Automation, and Test in Europe), with Rodric Rabbah (IBM).

10.1.2.2. Member of Conference Program Committees

Tomofumi Yuki was a program committee member for the RST Track (Reliable Software Technologies and Communication Middleware) of SAC’16 (31st ACM Symposium on Applied Computing).

Paul Feautrier was a member of the program committees of IMPACT’15, IMPACT’16, and PECCS’15 (5th International Conference on Pervasive and Embedded Computing and Communication Systems).

Christophe Alias was a member of the program committee of IMPACT’16.

Alain Darté was a member of the program committees of PACT’15 (International Conference on Parallel Architectures and Compilation Techniques) and X10’15 (international workshop on X10, part of PLDI’15).

10.1.2.3. Reviewer

Paul Feautrier was a reviewer for IMPACT’15, IMPACT’16, PARCO’15, and PACT’15.

Tomofumi Yuki was a reviewer for PACT’15 and X10’15.

Christophe Alias was a reviewer for DATE’15.

Laure Gonnord was a reviewer for VMCAI’15, CGO’15, and PARCO’15.

Alain Darté was a reviewer for DATE’15, IMPACT’15, X10’15, and PACT’15.

10.1.3. Journal

10.1.3.1. Member of Editorial Boards

Paul Feautrier is a member of the editorial board of IJPP, the “International Journal of Parallel Programming”.

10.1.3.2. Reviewer - Reviewing Activities

Paul Feautrier was reviewer for “Information and Computation”, ACM TODAES, ACM TOPLAS, and IJPP.

Tomofumi Yuki was reviewer for the PARCO journal.

Alain Darté was reviewer for the ACM TACO journal and the “Software Practice and Experience” journal.

Christophe Alias was reviewer for Parallel Computing and IEEE TVLSI.

10.1.4. Invited Talks

Paul Feautrier was invited to give a talk on “The Numerical Solution of the Transfer Equation”, at a workshop in honor of Roger Cayrel, Paris Observatory, Dec. 2015.

In June 2015, Laure Gonnord was invited at Google, Mountain View and SRI, to give talks about her research about static analyses for compilers.

10.1.5. Scientific Expertise

Alain Darté was invited to be part of the scientific committee of the CPU (“certification numérique et fiabilité”) cluster of excellence (from Bordeaux Idex), and its internal evaluation in Sep. 2015.

In 2015, Maroua Maleej has produced 7 Research Tax Credit documents for Accenture group France as a scientific consultant. The goal is to expertise research done by Accenture project-teams and suggest further ideas by evaluating the state of the art.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence:

- Laure Gonnord: Architecture des ordinateurs (TD+TP=40h), L2, Université Lyon 1 Claude Bernard: Spring 2015.
- Maroua Maleej: Algorithmique et Programmation Fonctionnelle et Récursive (TP=28h), L1, Université Lyon 1 Claude Bernard: Fall 2015.
- Christophe Alias: Introduction à la compilation (CM+TD=24h), L3, INSA Centre-Val-de-Loire: Spring 2015.
- Christophe Alias: Concours E3A—épreuve informatique MPSI (correcteur): Spring 2015.

Master:

- Laure Gonnord, Program Analysis and Verification (CM 24h), M1, Ecole Normale Supérieure de Lyon. With David Monniaux.
- Laure Gonnord, Compilation (TP 28h), M1, Ecole Normale Supérieure de Lyon.
- Laure Gonnord, Introduction aux systèmes et réseaux (CM/TP 52h), M2 Pro, Université Lyon 1.
- Laure Gonnord, Compilation (TD/TP 24h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord, Complexité (TD 15h), M1, Université Lyon 1 Claude Bernard.
- Laure Gonnord, Temps Réel (TP 24h), M1, Université Lyon 1 Claude Bernard.
- Christophe Alias, Optimisation d’applications embarquées (CM+TD=18h), M1, INSA Centre-Val-de-Loire.

- Christophe Alias, Advanced Compilers: Loop Transformations and High-Level Synthesis (CM 8h), M2, Ecole Normale Supérieure de Lyon.
- Christophe Alias, Compilation (CM 16h), M1, Ecole Normale Supérieure de Lyon.
- Tomofumi Yuki and Christophe Alias, Advanced Compilers: Loop Transformations and High-Level Synthesis, 24h, M2, ENS Lyon.

Master school:

- Laure Gonnord organized in Jan. 2015 a research school entitled “Static analyses in the state-of-the-art compilers” (invited speaker: Fernando Pereira). See http://laure.gonnord.org/pro/research/compil_research_school.html

EJCP:

Tomofumi Yuki has given a one-day lecture at the École Jeunes Chercheurs en Programmation 2015. See <http://ejcp2015.inria.fr/>.

10.2.2. Supervision

PhD in progress: Guillaume Iooss, “Semantic tiling”, started in September 2011, joint PhD ENS-Lyon/Colorado State University, advisors: Christophe Alias and Alain Darté (ENS-Lyon) / Sanjay Rajopadhye (Colorado State University).

PhD in progress: Alexandre Isoard, “Streaming-related code optimizations”, started in September 2012, advisor: Alain Darté.

PhD in progress: Maroua Maleej, “Low cost static analyses for compilers”, started in October 2014, advisors : Laure Gonnord and Alain Darté, then Laure Gonnord and Frédéric Vivien (Roma team).

10.2.3. Juries

Paul Feautrier was a member of the defense committee of the PhD of Alexis Foulhié (Grenoble, Oct. 2015), entitled “Revisiting the abstract domain of polyhedra: constraints-only representation and formal proof”, and was a reviewer for the HDR thesis of Corinne Ancourt (UPMC, May 2015), entitled “Sûreté: de l’analyse à l’instrumentation et à la synthèse de code”.

Laure Gonnord was a member of the doctoral committee for the evaluation of the first year of the PhD of F. Maurica, Université de la Réunion, in Dec. 2015.

Alain Darté was the reviewer of the PhD of Gergö Barany (Technische Universität Wien, Austria, March 2015), entitled “Integrated Code Motion and Register Allocation”.

10.3. Popularization

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

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

CORSE Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- Fabrice Rastello: Publication Chair ACM/IEEE CGO 2015
- Fabrice Rastello: Steering Committee Journées française de la compilation
- Fabrice Rastello: Steering Committee ACM/IEEE CGO
- Frédéric Desprez: Steering committee for the ISC Cloud & Big Data conference 2015
- Frédéric Desprez: General chair of VTDC 2015 (workshop within HPDC 2015)
- Ylies Falcone: Chair of the second international competition on Runtime Verification (CRV 15)

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- Fabrice Rastello: Program Chair ACM/IEEE CGO 2016
- Frédéric Desprez: Program co-chair BigDataCloud'2015 (workshop within EuroPAR 2015)
- Frédéric Desprez: Global chair of topic "Grid, Cluster and Cloud Computing" within EuroPAR 2015

9.1.2.2. Member of the conference program committees

- Fabrice Rastello: ACM/IEEE CGO 2016
- Fabrice Rastello: CRI 2015
- Alain Ketterlin: ACM/IEEE CGO 2016
- Frédéric Desprez: ACM/IEEE CCGrid 2015
- Frédéric Desprez: CLOSER 2015
- Frédéric Desprez: Workshop Committee at the 2015 ACM/IEEE Supercomputing Conference 2015
- Frédéric Desprez: IEEE CAC 2015
- Frédéric Desprez: IEEE Cluster 2015
- Ylies Falcone SAC-SVT 2015
- Ylies Falcone IPAC 2015
- Ylies Falcone CRI 2015
- Ylies Falcone MSR 2015
- Ylies Falcone PCODA 2015

9.1.2.3. Reviewer

- François Broquedis: EUROPAR 2015, SAC 2015
- Brice Videau: EUROPAR 2015, SAC 2015, IPDPS 2015, COMPASS 2015
- Ylies Falcone MSR 2015, RV 2015, ASE 2015, OOPSLA 2015, FM 2015, CAV 2015, DAC2015, DATE 2015

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

- Fabrice Rastello: ACM TACO, ACM TOCS

- François Broquedis: ACM TACO
- Brice Videau: ACM TACO, PARCO, JPDC
- Kevin Pouget: ACM TACO
- Frédéric Desprez: JPDC
- Frédéric Desprez: Journal of Supercomputing
- Ylies Falcone 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, ACM Transaction on Aspect-Oriented Development, The Computer Journal, ACM Transactions on Information and System Security, Elsevier Computer Review, Software Testing, Verification and Reliability.

9.1.4. Invited talks

- HiPEAC ACACES Summer School 2015 (teacher): “SSA-based Compiler Design”
- Fabrice Rastello: LLNL, Apple Dec 2015: “Toward Automatic Characterisation of the Data Access Complexity of Programs”
- Frédéric Desprez: Inria/EPFL Workshop, Jan. 2015: “Grid’5000: Running a Large Instrument for Parallel and Distributed Computing Experiments”
- Jean-François Méhaut, Maison de la simulation, Saclay, France, March 2015: “BOAST: Un environnement de metaprogrammation pour une génération de code portable et efficace des noyaux de calcul HPC”
- Jean-François Méhaut, Laboratoire Jacques-Louis Lions, Paris, France, Journées inaugurales de la machine de calcul, June 2015: “BOAST: Programmation des noyaux de calcul pour les projets européens Mont-Blanc”
- Jean-François Méhaut, Federal University of Santa Catarina, Florianopolis, Brazil, October 2015: “CORSE: Compiler Optimizations and Runtime Systems”

9.1.5. Scientific expertise

- Frédéric Desprez: Referee for the Research Council of Norway
- Frédéric Desprez: ANR
- Frédéric Desprez: Reviewer for a project within the FET Initiatives in FP7 of the European Commission
- 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 Méhaut Eurolab-4-HPC EU action, member of the panel

9.1.6. Research administration

- Frédéric Desprez: Deputy Scientific Director at Inria
- Frédéric Desprez: Director of the GIS GRID5000

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Fabrice Rastello (external intervention), Programming Languages and Compiler Design, 3 hours, M1 of international MoSIG, UJF, Grenoble, France

Master and PhD: Jean-François Méhaut, Parallel Programming, 40 hours, University of Yaoundé 1, LIRIMA, CETIC, February 2015

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

L3, Jean-François Méhaut, Numerical Methods, 50 hours, Polytech Grenoble,
 M1, Jean-François Méhaut, Operating System Project, 20 hours, UFR IM2AG
 L3, Jean-François Méhaut, Advanced Algorithm, 50 hours, UFR IM2AG
 L3, François Broquedis, Introduction to algorithms and programming, 80 hours, Grenoble Institute of Technology (ENSIMAG)
 L3, François Broquedis, Introduction to UNIX, 20 hours, Grenoble Institute of Technology (ENSIMAG)
 L3, François Broquedis, C programming, 50 hours, Grenoble Institute of Technology (ENSIMAG)
 M1, François Broquedis, Operating Systems and Parallel Programming, 20 hours, Grenoble Institute of Technology (ENSIMAG)
 M1, François Broquedis, Operating Systems Project, 20 hours, Grenoble Institute of Technology (ENSIMAG)
 M2, François Broquedis, Parallel and Distributed Programming, Grenoble Institute of Technology (ENSIMAG)
 Master, Florent Bouchez Tichadou, Compilation project, 15.5 hours, M1 Info & M1 MoSig, UFR IM2AG
 Licence, Florent Bouchez Tichadou, C programming, 33 hours, L3, Grenoble Institute of Technology (ENSIMAG)
 Master, Florent Bouchez Tichadou, Algorithms and Program Design, 33 hours, M1 MoSIG, UFR IM2AG
 Licence, Florent Bouchez Tichadou, Algorithms languages and programming, 71 hours, L2, UFR IM2AG
 Master, Florent Bouchez Tichadou, Operating Systems, 28.5 hours, M1 Info, UFR IM2AG
 Master, 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 in progress: Duco van Amstel, Scheduling and optimization for memory locality of dataflow programs on many-core processors, April 1st 2013, advised by Fabrice Rastello and Benoit Dupont-de-Dinechin

PhD in progress: Diogo Sampaio, Profiling Guided Hybrid Compilation, October 8 2013, advised by Fabrice Rastello

PhD in progress: François Gindraud, Semantics and compilation for a data-flow model with a global address space and software cache coherency, January 1st 2013, advised by Fabrice Rastello and Albert Cohen.

PhD in progress: Venmugil Elango, Dynamic Analysis for Characterization of Data Locality Potential, September 2010, advised by Fabrice Rastello and P. Sadayappan.

9.2.2.2. Jean-François Méhaut

PhD in progress: Serge Emteu, CIFRE ST Microelectronics, advised by Miguel Santan (STM), Alexandre Termier (Dream/Irisa), Jean-François Méhaut

PhD in progress: Oleg Iegorov, advised by Alexandre Termier (Dream/Irisa) and Jean-François Méhaut

PhD in progress: Nassim Halli, CIFRE with Asselta, advised by Henri-Pierre Charles (CEA/DRT List, CRI PILSI), Jean-François Méhaut

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

9.2.2.3. Frédéric Desprez

PhD in progress: 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

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), Raymond Namyst (Inria/STORM), Bruno Raffin (Inria/MOAIS), François Broquedis

Engineer internship: Olivier Soldano, *Efficient execution of OpenMP applications: a compiler/runtime cooperation*, co-advised by Jean-François Méhaut and François Broquedis

9.2.2.5. Ylies Falcone

PhD in progress: Antoine El-Hokayem, *Decentralised and Distributed Monitoring of Cyber-Physical Systems*

PhD defended: Abdurrahman Pektas, *Behavior based malware classification using online machine learning*, co-advised by Jean-Claude Fernandez (Vérimag)

9.2.3. Juries

9.2.3.1. Fabrice Rastello

Emmanuelle Saillard, Reviewer, *Static/Dynamic Analyses for Validation and Improvement of Multi-models HPC Applications*, PhD of the University of Bordeaux, 24/05/15

9.2.3.2. Jean-François Méhaut

PhD: Ashraf Elantably, *Study of task migration in a multi-tiles architecture: Automatic generation of an agent based solution*, Université de Grenoble, TIMA, 16/12/2015

PhD: Pei Li, *Système Unifié de transformation de code et d'exécution pour un passage aux architectures multi-coeurs hétérogènes*, Université de Bordeaux, Inria/Storm, Telecom SudParis, 17/12/2015

PhD: Anastasia Butko, *Fast Cycle-approximate Simulation Techniques for Manycore Architecture Exploration*, Université de Montpellier, LIRMM, 10/12/2015

PhD: Fabien Rozar, *Contributions à l'amélioration de l'extensibilité de simulations parallèles de plasmas turbulents*, Université de Bordeaux, CEA Cadarache, Maison de la simulation Saclay, 5/11/2015

PhD: Mohamed Bergach, *Adaptation de la Transformée de Fourier rapide sur une architecture mixte CPU/GPU intégrée*, Université de Nice Sophia Antipolis, 2/10/2015

PhD: Andi Drebes, *Dynamic Optimization of Data-flow task-parallel applications for large scale NUMA systems*, Université Pierre et Marie Curie, 25/6/2015

PhD: Corentin Rossignon, *Un modèle de programmation à grain fin pour la parallélisation de solveurs linéaires creux*, Université de Bordeaux, Inria/Storm, Total, 17/07/2015

PhD: Abal Cheick Ahamed, *Méthodes Numériques pour la résolution accélérée des systèmes linéaires de grandes tailles sur architectures hybrides massivement parallèles*, Ecole Centrale de Paris, 7/7/2015

HDR: Patrick Carribault, *Compiler/Runtime Cooperation for Multi-Paradigm Parallelism*, Université de Versailles Saint Quentin en Yveline, CEA Bruyères, 8/7/2015

HDR: Marc Perache, *Vers des supports exécutifs et des outils de profilage adaptés aux architectures many/multi coeurs dans le cadre du calcul hautes performances*, Université de Versailles Saint-Quentin en Yvelines, CEA Bruyères, 3/11/2015

9.2.3.3. Frédéric Desprez

PhD: Xavier Lacoste, Reviewer, *Scheduling and memory optimizations for sparse direct solver on multi-core/multi-gpu cluster systems*, Université de Bordeaux, 18/02/15

PhD: Sylvain Gault, *Improving MapReduce Performance on Clusters*, Ecole normale supérieure de Lyon, 23/03/15

HDR: Philippe Merle, Reviewer, *Intergiciel d'intergiciels adaptable à base de Services, Composants et Aspects*, Université de Lille3, 24/09/15

PhD: Emmanuel Cieren, Reviewer, *Molecular Dynamics for Exascale Supercomputers*, Université de Bordeaux, 09/10/15

PhD: Astrid Casadei, *Optimisations des solveurs linéaires creux hybrides basés sur une approche par complément de Schur et décomposition de domaine*, Université de Bordeaux, 19/10/15

HDR: Sébastien Monnet, *Contributions à la réplique de données dans les systèmes distribués à grande échelle*, Université Pierre et Marie Curie, 03/11/15

HDR: Georges Da Costa, *Évaluation et optimisation de performance énergétique des centres de calcul*, Université de Toulouse 3 Paul Sabatier, 12/11/15

HDR: Patricia Stolf, Reviewer, *La gestion des ressources pour des infrastructures vertes par la reconfiguration*, Université de Toulouse 3 Paul Sabatier, 13/12/15

PhD: Florent Lopez, *Solveur multifrontal QR à base de tâches pour architectures hétérogènes*, Université de Toulouse 3 Paul Sabatier, 11/12/15

9.2.3.4. Ylies Falcone

PhD: reviewer of the thesis of Eric Lupaud Ngoupé (University of Québec at Chicoutimi).

PhD: examiner of the thesis of Srinivas Pinisetty (Inria Rennes) on *Runtime Enforcement of Timed Properties*

DREAMPAL Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

F. Guyomarch, P. Marquet and S. Meftali were members of the ComPAS 2015 organizing committee (Lille, 2015).

F. Guyomarch and S. Meftali were members of the Archi summer school organizing committee (Lille, 2015).

9.1.2. Scientific events selection

9.1.2.1. responsable of the conference program committee

S. Meftali was responsible of the ComPAS 2015 conference program committee.

9.1.2.2. Member of the conference program committees

J.-L. Dekeyser was member of the ComPAS 2015 conference program committee and is member in the Reconfig 2016 and ReCoSoc 2016 program committees.

F. Guyomarch is member of the ComPAS 2016 program committee, which will take place in Lorient (<http://compas2016.sciencesconf.org>).

V. Rusu is member of the WRLA 2016 program committee, which will take place in Eindhoven (<https://fmse.info.uaic.ro/events/WRLA2016/>).

9.1.3. Research administration

V. Rusu is elected member of the Inria evaluation committee.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

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

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

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

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

Licence : Samy Meftali, Architecture des ordinateurs, 75h, L2, UFR IEEA, Université Lille 1, France

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

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

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

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

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

Licence : F. Guyomarch, Algorithmique et programmation, 72h, L1, IUT-A (Univ. Lille 1)

Licence : F. Guyomarch, Conception de sites web, 8h, L1, IUT-A (Univ. Lille 1)

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

Licence : F. Guyomarch, Algorithmique avancée, 44h, L2, IUT-A (Univ. Lille 1)

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

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

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

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

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

Licence : V. Rusu, Logique , 30h, M1, UFR IEEA, (Univ. Lille 1)

Master : V. Rusu, Architecture avancée des ordinateurs, 36h, M1, UFR IEEA, (Univ. Lille 1)

9.2.2. Supervision

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

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

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

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

9.3. Popularization

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

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

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

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

POSTALE Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- Marc Baboulin,
 - Member of the steering committee of HPC 2015
 - Minisymposium “Randomized algorithms in numerical linear algebra.” Organizers: Marc Baboulin, Jack Dongarra (Univ. of Tennessee) et Sherry Li (Lawrence Berkeley National Laboratory), SIAM Conference on Computational Science and Engineering, Salt Lake City, USA, March 14-18, 2015.
- Christine Eisenbeis, comité d’organisation du colloque "Les métiers du travail scientifique : images et valeurs, réalités et défis", 20-21 mai 2015, Orsay, (<http://www.centre-dalembert.u-psud.fr/2015-les-metiers-du-travail-scientifique-images-et-valeurs-realites-et-defis/>).

9.1.2. Journal

9.1.2.1. Member of the editorial board

- Christine Eisenbeis, IJPP

9.1.3. Invited talks

- Marc Baboulin, invited plenary speaker at the HPCSE conference, Solan, Czech Republic, May 25-28, 2015.

9.1.4. Scientific expertise

- Marc Baboulin, comité de sélection pour un poste de maître de conférences en informatique, université Paris-Sud 11, mai 2015.
- Christine Eisenbeis, comité de sélection pour un poste de professeur d’informatique, université Paris-Sud 11, mai 2015.
- Joël Falcou, comité de sélection pour un poste de maître de conférences en informatique, université Paris-Sud 11, mai 2015.
- Lionel Lacassagne, comité de sélection pour un poste de maître de conférences en informatique, université Paris-Sud 11, mai 2015.

9.2. Teaching - Supervision - Juries

9.2.1. Supervision

PhD in progress: Lénaïc Bagnères, "Adaptation automatique et semi-automatique des optimisations de programmes", University Paris-Sud 11, supervisors: Cédric Bastoul and Christine Eisenbeis

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

PhD defended: Jason Lambert, "Parallélisation de simulations interactives de champs ultrasonores pour le contrôle non destructif", CEA List/Disc funding, University Paris-Sud 11, July 3rd, 2015, Supervisor: Lionel Lacassagne

PhD defended: Adrien Rémy, "Solving dense linear systems on accelerated multicore architectures", University Paris Sud 11, July 8th, 2015, Supervisors: M. Baboulin and B. Rozoy

PhD defended: Antoine Tran Tan, "Squelettes algorithmiques asynchrones : application aux langages orientés domaine", University Paris-Sud 11, October 8th, 2015, Supervisor: Joël Falcou

PhD defended: Yushan Wang, "Solving Incompressible Navier-Stokes Equations on Heterogeneous Parallel Architectures", University Paris Sud 11, April 9th, 2015, Supervisors: M. Baboulin and O. Le Maître

9.2.2. *Juries*

- Marc Baboulin,
 - PhD defence of Michele Mangili, Politecnico di Milano (15/12/2015), chairman of the committee.
 - HDR defence of Stéphane Louise, CEA Saclay (29/06/2015), chairman of the committee.
- Christine Eisenbeis, rapporteuse de la thèse de Nicolas Triquenaux, « Energy Characterization and Savings in Single and Multiprocessor Systems : Understanding how much can be saved and how to achieve it in modern systems » , 18 septembre 2015, université de Versailles-Saint-Quentin.

9.3. Popularization

Christine Eisenbeis est membre du conseil scientifique des programmes du centre d'Alembert, Centre Interdisciplinaire d'Étude de l'Évolution des Idées, des Sciences et des Techniques (CIEEIST), de l'université Paris-Sud. À ce titre, elle a fait partie du comité d'organisation du colloque "Les métiers du travail scientifique : images et valeurs, réalités et défis", 20-21 mai 2015, Orsay, (<http://www.centre-dalembert.u-psud.fr/2015-les-metiers-du-travail-scientifique-images-et-valeurs-realites-et-defis/>).

TASC Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events selection

10.1.1.1. Chair of conference program committees

- **Nicolas Beldiceanu**: Sixth International Workshop on Bin Packing and Placement Constraints.

10.1.1.2. Member of the conference program committees

- **Nicolas Beldiceanu**: Member of the senior program committee of **CP 2015**.
- **Nicolas Beldiceanu**: Member of the program committee of **CP 2016**.
- **Nicolas Beldiceanu**: Member of the senior program committee of **CPAIOR 2015**.
- **Nicolas Beldiceanu**: Member of the senior program committee of **CPAIOR 2016**.
- **Nicolas Beldiceanu**: Member of the program committee of **IJCAI 2015**.
- **Xavier Lorca**: Member of the program committee of **IJCAI 2015**.
- **Xavier Lorca**: Member of the program committee of **CP 2015**.
- **Xavier Lorca**: Member of the program committee of **ROADEF 2015**.
- **Xavier Lorca**: Member of the program committee of **ROADEF 2016**.
- **Eric Monfroy**: Track chair de **ACM-SAC 2015** CSP track.
- **Eric Monfroy**: Member of the program committee of **Evocop 2015**.
- **Eric Monfroy**: Member of the program committee of **Evocop 2016**.
- **Eric Monfroy**: Member of the program committee of **IJCAI 2015**.
- **Eric Monfroy**: Member of the program committee of **ICTAI 2015**, special track on SAT and CSP.
- **Eric Monfroy**: Member of the program committee of **JFPC 2015**.
- **Florian Richoux**: Member of the program committee of **LION 9**.
- **Florian Richoux**: Member of the program committee of **SAC 2015**.
- **Florian Richoux**: **Journé Jeux Vidéo and Intelligence Artificielle 2015**.

10.1.1.3. Reviewer

- **Nicolas Beldiceanu**, reviewer at **CPAIOR 2015**.
- **Nicolas Beldiceanu**, reviewer at **CP 2015**.
- **Nicolas Beldiceanu**, reviewer at **CPAIOR 2016**.
- **Nicolas Beldiceanu** reviewer at **AAAI 2016**.
- **Florian Richoux** reviewer at **IEEE Transactions on Comp. Int. and AI in Games**.
- **Florian Richoux** reviewer at **AIIDE 2015** (Artificial Intelligence and Interactive Digital Entertainment).
- **Florian Richoux** reviewer at Artificial Intelligence in Adversarial Real-Time Games workshop associated to **AIIDE 2015**.

10.1.2. Journal

10.1.2.1. Member of the editorial boards

- **Nicolas Beldiceanu**, **Constraints** (Springer).

- [Thierry Petit](#), [Constraints \(Springer\)](#).
- [Florian Richoux](#), [Encyclopedia of Computer Graphics and Games \(Springer\)](#).
- [Charlotte Truchet](#), blog [Binaire](#) of [lemonde](#).

10.1.2.2. Reviewer - Reviewing activities

- [Xavier Lorca](#) reviewer at [AIJ](#).
- [Xavier Lorca](#) reviewer at [Constraints \(Springer\)](#).
- [Xavier Lorca](#) reviewer at [RAIRO](#).

10.1.3. Invited talks

- [Florian Richoux](#) *Feedback on IA competitions in the context of games*. Workshop PFIA 2015, Jeux Vidéo and IA, July 2015, Inria Rennes (France).
- [Florian Richoux](#) *Antagonist IA for Win That War !*, workshop PFIA 2015, Jeux Vidéo and IA, July 2015, Inria Rennes (France).

10.1.4. Leadership within the scientific community

[Xavier Lorca](#) is the co-head of the [OR and Constraints](#) working group.

10.1.5. Research administration

Within the forthcoming research unit *UMR LS2N* [Xavier Lorca](#) is the co-head of the cluster *Data Science and Decision* that group together seven research teams.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Master: [Nicolas Beldiceanu](#), Constraint ([Master ORO](#)), 30h, M2, [Nantes University](#), France.
- Master: [Nicolas Beldiceanu](#), Logic Programming, 32h, M2, [Mines Nantes](#), France.
- Master: [Nicolas Beldiceanu](#), Gipad end project, 8h, M2, [Mines Nantes](#), France.
- Licence: [Nicolas Beldiceanu](#), Programming with Java, 42h, L3, [Mines Nantes](#), France.
- Licence: [Nicolas Beldiceanu](#), Automata, 12h, L3, [Mines Nantes](#), France.
- Licence: [Nicolas Beldiceanu](#), IPIPIP project, 12h, L1, [Mines Nantes](#), France.
- Licence: [Gilles Chabert](#), Variational calculus, 12h, L3, [Mines Nantes](#), France.
- Licence: [Gilles Chabert](#), Numerical methods, 21h, L3, [Mines Nantes](#), France.
- Master: [Gilles Chabert](#), Project Supervision, L3, Master 1 and Master2, [Mines Nantes](#), France.
- Master: [Gilles Chabert](#), Non-linear optimization, 20h, M1, [Mines Nantes](#), France.
- Master: [Gilles Chabert](#), Non-linear optimization, 24h, M1, [Nantes University](#), France.
- Master: [Gilles Chabert](#), Non-linear programming, 20h, M2, [Mines Nantes](#), France.
- Licence: [Xavier Lorca](#), Software engineering and miscellaneous , 30h, [Mines Nantes](#), France.
- Master: [Xavier Lorca](#) In charge of the organisation of the Gipad specialty (coordinating 12 modules of 45h each).
- Master: [Xavier Lorca](#) Gipad (Graph and Algorithms, Artificial Intelligence and Constraint Programming, Decision Analytics, Data Visualisation, Architecture of Computer System and Software), 100h, [Mines Nantes](#), France.
- Licence, Master: [Eric Monfroy](#), Head of the computer science department, [Nantes University](#), France.
- Licence: [Eric Monfroy](#), Logic, L2 [Nantes University](#), France.
- Licence: [Eric Monfroy](#), Computer Architecture, L3 [Nantes University](#), France.

Licence: **Eric Monfroy**, Computability theory and foundations, L3 **Nantes University**, France.
 Master: **Eric Monfroy**, Modelling with constraints, (Master ORO), M1, **Nantes University**, France.
 Licence: **Florian Richoux**, Algorithm and data structures, L2, **Nantes University**, France.
 Licence: **Florian Richoux**, Object programming and design patterns, L3, **Nantes University**, France.
 Licence: **Florian Richoux**, Operation Research, exercises and practice, L3, **Nantes University**, France.
 Master: **Florian Richoux**, Machine Learning, exercises and practice (Master ATAL), M1, **Nantes University**, France.
 Master: **Florian Richoux**, Constraint programming (Master ORO), M1, **Nantes University**, France.
 Licence: **Charlotte Truchet**, 192h, L1, **Nantes University**, France.

10.2.2. Supervision

PhD : **Alban Derrien**, Cumulative scheduling in constraint programming (energetic characterization of reasoning and robust solutions), **Mines Nantes**, November 27 2015, **Thierry Petit** and **Nicolas Beldiceanu**.
 PhD in progress : **Ignacio Salas Donoso**, Packing curved shapes, May 2013, **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.
 PhD in progress : **Léopold Houdin**, Set-based algorithms for characterizing limit cycles in bio-inspired robotics, October 2015, **Frédéric Boyer**, **Gilles Chabert**, **Alexandre Goldsztejn**.
 Master thesis : Ekaterina Arafailova (February-June 2015), *reformulation of automata with accumulators as linear programs*, **Nicolas Beldiceanu**.
 Master thesis : Julien Fradin (February-June 2015), *extensions to the GHOST library*, **Florian Richoux**.
 Master thesis : Adrien Bodineau (January-April 2015), *extensions to the GHOST library*, **Florian Richoux**.
 Internship : Guillaume Legru (April-May 2015), *IA for combat games*, **Florian Richoux**.

10.2.3. Juries

- **Nicolas Beldiceanu**, Member of the committee of the PhD of **Alban Derrien**, Cumulative scheduling in constraint programming (energetic characterization of reasoning and robust solutions), **Mines Nantes**, November 27 2015.
- **Nicolas Beldiceanu**, Member of the committee of the PhD of **Haykel Boukadida**, Automatic creation of video summarisation with constraint programming, **Rennes University**, December 4 2015.
- **Xavier Lorca**, Member of the committee of the PhD of **Alban Derrien**, Cumulative scheduling in constraint programming (energetic characterization of reasoning and robust solutions), **Mines Nantes**, November 27 2015.

- **Xavier Lorca**, Member of the committee of the PhD of **Nebras Gharbi**, Compression and parallelisation in CSP, **Lens University**, December 4 2015.
- **Xavier Lorca**, Member of the committee of the PhD of **Mohammed Rezgui**, Parallelism in constraint programming, **Nice University**, July 7 2015.
- **Eric Monfroy**, Member of the committee of the PhD of **Roberto Amadini**, Portfolio Approaches in Constraint Programming, **Bologna University**, June 4 2015.
- **Thierry Petit**, Member of the committee of the PhD of **Alban Derrien**, Cumulative scheduling in constraint programming (energetic characterization of reasoning and robust solutions), **Mines Nantes**, November 27 2015.

10.3. Popularization

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

AOSTE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. Member of the organizing committees

- Liliana Cucu: Dagstuhl seminar on Mixed Criticality Systems
- Robert Davis: Dagstuhl seminar on Mixed Criticality Systems

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

- Liliana Cucu: RTNS2015, WMC2015
- Robert Davis: RTAS2016, WMC2015

10.1.2.2. Member of the conference program committees

- Robert de Simone: EmSoft'2015, FDL'2015, Memocode'2015.
- Yves Sorel: RTNS 2015, DASIP 2015, EMSOFT 2015.
- Frédéric Mallet: DATE'2015, MoDELS'2015, MSR'2015, ESLsyn'2015, ICTERI'2015, FDL'2015
- Julien Deantoni: DAC'2015, MiSE'2015, GEMOC'2015
- Liliana Cucu: RTAS2015, ETFA2015, SIES2015, MISTA2015, DATE2015 and MAPSP2015
- Dumitru Potop Butucaru: RTNS 2015, LCTES 2015, ESLSyn 2015
- Adriana Gogonel: ACM RACS2015, RTNS2015 and WMC2015
- Dorin Maxim: DATE2015 and RTNS2015

10.1.3. Journal

10.1.3.1. Member of the editorial boards

- Yves Sorel: Traitement du Signal Journal, Real-Time System Journal

10.1.4. Invited talks

- Frédéric Mallet: International Summer School on Methods and Tools for the Design of Digital Systems, Bremen
- Liliana Cucu: VECOS2015

10.1.5. Scientific expertise

- Yves Sorel: Steering Committees of the System Design and Development Tools Group of Systematic Paris-Region Cluster, and of the Technologies and Tools Program of SystemX Institute for Technological Research
- Robert de Simone: Board of Administrators of CIM-France Design Platform.

10.1.6. Research administration

- Robert de Simone is member of the Board of the UNS Doctoral School EDSTIC.
- Liliana Cucu is member of Inria Evaluation Commission.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

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

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

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

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

Master: 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, Ingénierie Dirigée par les modèles par la pratique, 24h, 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, 56h, U. Dunarea de Jos, Romania

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

10.2.2. Supervision

PhD: Mohamed Bergach, *Adaptation of the Fast Fourier Transform processing on hybrid integrated CPU/GPU architecture*, UNS, defended October 2015.

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

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

PhD in progress: 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 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.

10.2.3. Juries

Robert de Simone: reviewer of Adrien Guatto (ENS Ulm), examiner of Andrea Enrici (Mines-Telecom Paris).

Frederic Mallet: reviewer of Judith Peters (U. Bremen, Germany), examiner (president) of Damian Vicino (Carleton University/U. Nice Sophia Antipolis).

Julien Deantoni: reviewer of Erwan Bousse (IRISA, University of Rennes)

Liliana Cucu: reviewer of Antoine Bertout (LIFL, November 2015)

Dumitru Potop Butucaru: examiner of José Echeveste (Université Pierre et Marie Curie/EDITE).

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 of MCC'2015 (*Model Checking Contest*). In 2015, he verified the forms describing the benchmark models and enhanced the format of these forms by adding new model properties. He contributed to the formalization of the contest's rules and to the writing of the two contest calls (call for models and call for tools). He also participated in migrating the PetriWeb model base (developed at the Technical University of Eindhoven) to the format and conventions of the contest. A journal article describing the achievements of the 5th Model Checking Contest has been written and submitted for publication.
- G. Salaün was a member of the organizing committee of SEFM'2015 (*13th International Conference on Software Engineering and Formal Methods*), York, United Kingdom, September 7–11, 2015.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- G. Salaün was programme committee co-chair of SVT-SAC'2015 (the *Software Verification Track of the Symposium on Applied Computing*), Salamanca, Spain, April 13–17, 2015.

9.1.2.2. Member of the conference program committees

- H. Garavel was program committee member of TACAS'2015 (*21th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*), London, United Kingdom, April 11–19, 2015.
- G. Salaün and W. Serwe were program committee members of FSEN'2015 (*6th International Conference on Fundamentals of Software Engineering*), Tehran, Iran, April 22–24, 2015.
- H. Garavel was program committee member of DCDS'2015 (*5th International Workshop on Dependable Control of Discrete Systems*), Cancun, Mexico, May 27–29, 2015.
- G. Salaün was program committee member of ICE'2015 (*8th Interaction and Concurrency Experience*), Grenoble, France, June 4-5, 2015.
- F. Lang, R. Mateescu, and W. Serwe were program committee members of FMICS'2015 (*20th International Workshop on Formal Methods for Industrial Critical Systems*), Oslo, Norway, June 22–23, 2015.
- G. Salaün was program committee member of WWV'2015 (*11th International Workshop on Automated Specification and Verification of Web Systems*), Oslo, Norway, June 23, 2015.
- F. Lang was program committee member of ETR'2015 (*École d'été Temps Réel*), Rennes, France, August 24–28, 2015.
- H. Garavel and G. Salaün were program committee members of SEFM'2015 (*13th International Conference on Software Engineering and Formal Methods*), York, United Kingdom, September 7–11, 2015.
- G. Salaün was program committee member of SCART'2015 (*1st International Workshop on the ART of Software Composition*), York, United Kingdom, September 8, 2015.
- G. Salaün was program committee member of FACS'2015 (*12th International conference on Formal Aspects of Component Software*), Rio de Janeiro, Brazil, October 14–16, 2015.

- H. Garavel was program committee member of MARS'2015 (*Workshop on Models for Formal Analysis of Real Systems*), Suva, Fiji, November 23, 2015.

9.1.2.3. Reviewer

- H. Garavel was a reviewer for CONCUR'2015 (*26th Conference on Concurrency Theory*), Madrid, Spain, September 1–4, 2015.
- R. Mateescu was a reviewer for FORTE'2015 (*35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems*), Grenoble, France, June 2–5, 2015.
- G. Salaün was a reviewer for SOCA'2015 (*8th IEEE International Conference on Service Oriented Computing and Applications*), Rome, Italy, October 19–21, 2015.
- W. Serwe was a reviewer for ATVA'2015 (*13th International Symposium on Automated Technology for Verification and Analysis*, October 12–15, 2015, Shanghai, China), MARS'2015, and TACAS'2016.

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*).
- G. Salaün is an editorial board member of SOCA (*Springer International Journal on Service Oriented Computing and Applications*).

9.1.3.2. Reviewer - Reviewing activities

- H. Garavel was a reviewer for the Mathematical Reviews (MathSciNet) of the American Mathematical Society.
- F. Lang was a reviewer for SOSYM (*International Journal on Software and Systems Modeling*).
- R. Mateescu was a reviewer for JISA (*Journal of Internet Services and Applications*), IEEE TSE (*Transactions on Software Engineering*), JLAMP (*Journal of Logical and Algebraic Methods in Programming*), FAoC (*Formal Aspects of Computing*), and STTT.
- G. Salaün was a reviewer for FAoC, JLAMP, JSS (*Journal of Systems and Software*), and MPE (*Mathematical Problems in Engineering*).

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, the PIC2LNT translator, and the PMC model checker (see § 5.2).

In 2015, the main facts are the following:

- We prepared and distributed twelve successive versions (2015-a to 2015-l) of CADP.
- We were requested to grant CADP licenses for 434 different computers in the world.

The CONVECS Web site⁰ was updated with scientific contents, announcements, publications, etc. Following a request from the computer staff of Inria Grenoble, we worked on the migration of the former Web site “<http://www.inrialpes.fr/vasy>” to a more recent web infrastructure. This former site was split into three new, distinct Web sites “<http://vasy.inria.fr>”, “<http://cadp.inria.fr>”, and “<http://fmics.inria.fr>”. Dedicated effort was made to properly redirect all former URLs so as not to create dead links.

By the end of December 2015, the CADP forum⁰, opened in 2007 for discussions regarding the CADP toolbox, had over 350 registered users and over 1600 messages had been exchanged.

Also, for the 2015 edition of the Model Checking Contest, we provided two families of models (totalling 15 Nested-Unit Petri Nets) derived from our LNT models.

⁰<http://convecs.inria.fr>

⁰<http://cadp.inria.fr/forum.html>

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

- The Ocarina tool for analysing AADL descriptions [58]
- The MIstRAL tool for middleware reconfiguration based on formal methods [61]
- The DFTCalc tool for analysing dynamic fault trees [49]
- The Vercors integrated environment for verifying and running distributed components [52]
- The IMCReo tool for Interactive Markov Chains in Stochastic Reo [60]
- The GROOVE tool for verification based on graph rewriting [54]

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

- Improving design patterns finder precision using model checking [34]
- Applying automata learning to embedded control software [62]
- Testing autonomous systems using communicating extended finite-state machines [32]
- Assisting refinement in system-on-chip design [59]
- Formal verification of plastic user interfaces exploiting domain ontologies [37]
- Action-based verification of a fire alarm system [35]

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

- G. Salaün gave a talk entitled “*Reliable Deployment, Reconfiguration, and Control of Cloud Applications*” on February 12, 2015 at the University of Málaga, Spain.
- H. Garavel gave a talk entitled “*Nested-Unit Petri Nets: A Useful Concept for PseuCo?*” on March 9, 2015 at Saarland University, Saarbrücken, Germany.
- W. Serwe gave a talk entitled “*Using a Formal Model to Improve Verification of a Cache-Coherent System-on-Chip*” on March 19, 2015 at the Cadence Club Formal, Grenoble, France.
- R. Mateescu gave a talk entitled “*Overview of MCL, a Data-Based Model Checking Language*” on March 31, 2015 at Inria Grenoble — Rhône-Alpes, Montbonnot, France.
- G. Salaün gave a talk entitled “*Reliable Deployment, Reconfiguration, and Control of Cloud Applications*” on March 26, 2015 at LIRMM, Montpellier, France.
- G. Salaün gave a talk entitled “*Reliable Deployment, Reconfiguration, and Control of Cloud Applications*” on April 2, 2015 at LABRI, Bordeaux, France.
- G. Salaün gave a talk entitled “*Verification of Asynchronously Communicating Systems*” on April 9, 2015 at IRISA, Rennes, France.
- H. Garavel gave a talk entitled “*Nested-Unit Petri Nets: Combining Hierarchy with Concurrency*” on May 6, 2015 at LIP6, Université Pierre et Marie Curie, Paris, France.
- G. Salaün gave a talk entitled “*Formal Modelling and Analysis of BPMN Processes*” on July 9, 2015 at XEROX, Meylan, France.
- F. Lang gave two talks entitled “*Vérification de systèmes concurrents asynchrones par des méthodes compositionnelles*” and “*CADP : une boîte à outils pour la construction et l’analyse de processus distribués*” on August 25, 2015 at ETR (*Ecole d’Été Temps Réel*), Rennes, France. He also held a lab session on CADP.
- G. Salaün gave a talk entitled “*Formal Modelling and Analysis of BPMN Processes*” on October 27, 2015 at the University of Málaga, Spain.

- H. Garavel gave a talk entitled “*Les aspects probabilistes dans CADP*” on December 8, 2015 at the “*Journées Inria*” held at LIP6, Université Pierre et Marie Curie, Paris, France.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

In 2015, we carried out the following teaching activities:

- G. Salaün is co-responsible of the ISI (*Ingénierie des Systèmes d’Information*) department of ENSIMAG since September 1, 2011.
- F. Lang gave a lecture on formal methods (6 hours) in the framework of the software engineering course given to the first year students of the MOSIG (Master of Science in Informatics at Grenoble).
- G. Salaün gave lectures (192 hours “*équivalent TD*”) to computer science engineering students of ENSIMAG (“*École Nationale Supérieure d’Informatique et de Mathématiques Appliquées*”, Grenoble INP) on “*Théorie des langages*” (first year), “*Programmation orientée objet*” (second year), and “*Modélisation et vérification de systèmes concurrents*” (third year). He also organized a series of “*Conférences technologiques*” (third year).
- H. Garavel, together with Laurence Pierre (TIMA, Grenoble), created a new curriculum “*High-confidence Embedded and Cyberphysical Systems*” of the international masters programme.

9.2.2. Supervision

- PhD: Hugues Evrard, “*Génération automatique d’implémentation distribuée à partir de modèles formels de processus concurrents asynchrones*”, Université Grenoble-Alpes, July 10, 2015, G. Salaün, F. Lang
- PhD: Abderahman Kriouile, “*Formal Methods for Functional Verification of Cache-Coherent System-on-Chip*”, Université Grenoble-Alpes, September 17, 2015, R. Mateescu, W. Serwe, M. Zendri
- PhD: Raquel Oliveira, “*Formal Specification and Verification of Interactive Systems with Plasticity: Applications to Nuclear-Plant Supervision*”, Université Grenoble-Alpes, December 3, 2015, H. Garavel, S. Dupuy-Chessa, G. Calvary, F. Lang
- PhD: Rim Sakka Abid, “*Coordination et Reconfiguration des Applications Distribuées Cloud*”, Université Grenoble-Alpes, December 16, 2015, G. Salaün, N. de Palma
- PhD in progress: Fatma Jebali, “*A Framework for the Formal Specification and Verification of Globally Asynchronous Locally Synchronous Systems*”, since December 2012, F. Lang, R. Mateescu
- PhD in progress: Gianluca Barbon, “*Debugging Concurrent Programs using Model Checking and Mining Techniques*”, since October 2015, G. Salaün

9.2.3. Juries

- H. Garavel was member of the jury for David Lugato’s habilitation thesis, entitled “*Formaliser par la modélisation : Applications au calcul haute performance et à la génération de tests par exécution symbolique*”, defended at Université de Bordeaux, France, on March 5, 2015.
- W. Serwe was PhD committee member for Zhen Zhang’s PhD thesis, entitled “*Verification Methodologies for Fault-Tolerant Network-on-Chip Systems*”, defended at University of Utah, Salt Lake City, USA, on October 26, 2015.

9.3. Popularization

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

The fifth conference ⁰, devoted to testing, held on June 16 in Toulouse and retransmitted by video-conference in Grenoble and Saclay, attracted participants from industry and academia. W. Serwe gave a talk (with Thierry Jérón, Inria Rennes), entitled “*TGV: Génération de tests de conformité à partir de modèles formels*”, and a talk (with Massimo Zendri, STMicroelectronics), entitled “*Génération de tests basés sur les modèles pour des systèmes sur puce avec cohérence de caches*”.

The sixth conference ⁰, devoted to safety, is to be held on January 26, 2016.

9.4. Miscellaneous Activities

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

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

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

H. Garavel is an expert evaluator for Minalogic “*pôle de compétitivité mondial*”.

H. Garavel was a reviewer for various ongoing ANR (*Agence Nationale de la Recherche*) pre-propositions and projects evaluated in 2015.

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

F. Lang is (together with Laurent Lefèvre from the AVALON Inria project-team) correspondent in charge of the 2014 and 2015 Inria activity reports at Inria Grenoble Rhône-Alpes.

E. Léo and W. Serwe are members of the “*Comité de centre*” of Inria Grenoble – Rhône-Alpes.

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

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

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

⁰<http://projects.laas.fr/IFSE/FMF/J5/index.html>

⁰<http://projects.laas.fr/IFSE/FMF/J5/index.html>

HYCOMES Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing committees

Benoît Caillaud has served on the program and organizing committees of LMCS 2015 (<http://www.acsysteme.com/fr/lmcs-2015>), a national workshop on mathematical modeling and scientific computing.

8.1.2. Scientific events selection

8.1.2.1. Member of the conference program committees

Benoît Caillaud has served on the program committee of ACSD 2015 (<http://www.ulb.ac.be/di/verif/pn2015acsd2015/>), a conference on the applications of concurrency in system design. He is a member of the steering committee of ACSD since 2006.

Albert Benveniste has served on the program committee of MODELICA 2015 (<https://www.modelica.org/events/modelica2015>), the conference on the Modelica mathematical modeling language.

8.1.2.2. Reviewer

Benoît Caillaud has reviewed papers submitted to the EMSOFT 2015, TACAS 2015 and ACC 2016 conferences.

8.1.3. Journal

8.1.3.1. Reviewer - Reviewing activities

Benoît Caillaud has reviewed papers submitted to Acta Informatica.

8.1.4. Invited talks

Benoît Caillaud has given an invited talk on *Time Domains in Hybrid Systems Modeling* at the LCCC-ACCESS workshop on Model-Based Engineering (<http://www.lccc.lth.se/index.php?page=LCCC-ACCESS-2015-05>). He has given an invited talk on *Contracts and Interfaces in System Engineering* at the CNRIA 2015 national conference (<http://cnria.cci.ucad.sn/>), Thiès, Sénégal.

Albert Benveniste has given invited talks at the Modelica 2015 conference (<https://www.modelica.org/events/modelica2015>) and at the GretsI 2015 colloquium (<http://www.gretsI.fr/colloque2015/>). He has given an invited talk at the LCCC-Access workshop on Model-Based Engineering (<http://www.lccc.lth.se/index.php?page=LCCC-ACCESS-2015-05>).

8.1.5. 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 editing the synthesis documents, regarding this department, used for the evaluation of IRISA by HCERES in January 2016.

8.2. Teaching - Supervision - Juries

8.2.1. 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.

8.2.2. Supervision

PhD in progress : Ayman Aljarbough, *Accelerated Simulation of Hybrid Systems*, started january 2014, supervised by Benoît Caillaud

8.2.3. Juries

Albert Benveniste has participated to the HdR jury of Axel Legay (University of Rennes 1, november 2015).

8.3. Popularization

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

MUTANT Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

MuTant team organized the **First Antescofo user Symposium** during **Ircam Forum Workshops** in November 2015 with 6 contributions and over 30 participants.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

Florent Jacquemard has participated in the program committee of the first International Conference on Technologies for Music Notation and Representation (TENOR 2015).

Jean-Louis Giavitto has participated in the program committee of the 41st International Computer Music Conference (ICMC), the ninth IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO), the International Workshop on Nature Inspired Cooperative Strategies for Optimization (NICSO), the 13th European Conference on Artificial Life (ECAL), the Digital Entertainment Technologies and Arts (DETA track at GECCO 2015, 10th International Conference on Information Processing in Cells and Tissues IPCAT, and TENOR 2015. He organized jointly with Gérard Berry the Réunion de l'inter-section des applications des sciences on "Informatique et Musique".

9.1.2.2. Reviewer

The members of the team participated as reviewers for IEEE ICASSP, ACM Multimedia Conferences, Sound and Music Computing, International Computer Music Conference (ICMC), Digital Audio Effects Conference (DAFx), IEEE Symposium on Logic In Computer Science (LICS), International Conference on Automated Deduction (CADE), Conference on Concurrency Theory (Concur), Computer Science Logic (CSL), Conference on Rewriting Techniques and Applications (RTA). and more.

9.1.3. Journal

9.1.3.1. Member of the editorial boards

Jean-Louis Giavitto is the redactor-in-chief of TSI (Technique et Science Informatiques) published by Lavoisier. He has coorganizd 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. This issue is finalized and will be printed in 2016.

9.1.3.2. Reviewer - Reviewing activities

The of the team participated as reviewers for the journal Information and Computation, ACM TOPLAS, IEEE Transactions on Multimedia, IEEE Transactions on Audio and Speech Signal Processing, and ACM Transactions on Intelligent Systems.

9.1.4. Invited talks

Jean-Louis Giavitto was invited to give the annual seminar of the Decanat des Science, Université de Namur (mai 2015) as well as at the International workshop *Mathemusical Conversations: mathematics and computation in performance and composition* jointly hosted by the Yong Siew Toh Conservatory of Music and the Institute for Mathematical Sciences in Singapore, in collaboration with the Center for Digital Music, Queen Mary University of London

9.1.5. Leadership within the scientific community

Arshia Cont is an elected board member of **International Computer Music Association (ICMA)** in charge of organizing the annual ICMC Conference and promoting research in the field.

9.1.6. Scientific expertise

Jean-Louis Giavitto is in the management team of the GDR GPL (Genie de la programmation et du logiciel), responsible with Etienne Moreau of the “Languages and Verification” pole of the GDR. He is also an expert for the ANR DEFI program and a reviewer for FET projects for the UC.

9.2. Teaching - Supervision - Juries

9.2.1. 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 in progress: Clément Poncelet, *Formal methods for analyzing human-machine interaction in complex timed scenario*. Started in october 2013, supervisor: Florent Jacquemard.
- PhD in progress: Philippe Cuvillier, *Probabilistic Decoding of strongly-timed events in realtime*, supervisor: Arshia Cont.
- 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.

9.2.2. Juries

Jean-Louis Giavitto was reviewer of the Habilitation of René Douence (Ecole des Mines de nantes, Composition non modulaire modulaire). He was examiners of the PhD thesis of Sergiu Ivanov (University of Paris Est, *Étude de la puissance d’expression et de l’universalité des modèles de calcul inspirés par la biologie*), and the PhD of Simon Martiel (University of Nice, *Approches informatique et mathématique des dynamiques causales de graphes*).

9.3. Popularization

Arshia Cont appeared as expert in **BFM Business TV** special live event on Music and New Technology.

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 was the general chair of the 20th ACM Conference on the Principles and Practice of Parallel Computing, PPOPP 2015, San Francisco (ranked A+). 186 participants. Coordination of the three co-located conferences. 700 participants.

Albert Cohen will be the general chair of the ACM Conference on Programming language Design and Implementation, PLDI 2017 conference in Barcelona (ranked A+). 600 participants expected.

9.1.1.2. Member of the organizing committees

Albert Cohen is in the steering committee of CC 2016, now separated from ETAPS. The number of submissions doubled after the renovation of the conference organization.

Albert Cohen is the sponsor chair of HiPEAC 2015 and 2016.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- Albert Cohen was program chair of the ARCS 2015 conference:
<http://arcs2014.itl.uni-luebeck.de>

9.1.2.2. Member of the conference program committees

- Timothy Bourke was a member of the PC of EMSOFT 2015, Modelica 2015, and RTAS 2016.
- Albert Cohen was a member of the PC of PLDI 2016, PACT 2016, 2015; IPDPS 2015; ICPP 2015 and of the ERC of PLDI 2015 (ranked A+); ASPLOS 2016 (ranked A+); ISCA 2016 (ranked A+);
- Marc Pouzet was a member of the PC of DAC 2015; EOOLT 2015; FLOPS 2015; and two french speaking conferences AFADL 2015 and MSR 2015. Member of the jury for “Prix de these GPL” (PhD thesis award in software engineering).
- Francesco Zappa Nardelli is a member of the PC of POPL 2016 and of the ERC of ECOOP 2015.

9.1.2.3. Reviewer

- Timothy Bourke was a reviewer for DAC 2015 (Design Automation Conference), DATE 2015 (Design, Automation and Test in Europe), ETAPS/FASE 2015 (Fundamental Approaches to Software Engineering), FLOPS 2015 (Symposium on Functional and Logic Programming), JFLA 2015 (Journées Francophones des Langages Applicatifs), and NFM 2015 (NASA Formal Methods Symposium).

9.1.3. Journal

9.1.3.1. Member of the editorial boards

- Albert Cohen is an Associate Editor of the ACM Transactions on Architecture and Code Optimization (TACO), since 2013.
- Albert Cohen is on the editorial board of the Int. Journal on Parallel Programming (IJPP, Springer), since 2011.

9.1.4. Invited talks

- February, T. Bourke presented “Exploiting and extending synchronous languages for hybrid modelling” at the MODPROD Workshop in Linköping, Sweden.
- February, T. Bourke presented “A synchronous approach to designing and compiling hybrid modelling languages” in the Chalmer’s Functional Programming group in Gothenburg, Sweden.
- February, T. Bourke presented “Mechanization of a mesh network routing protocol and the proof of its loop freedom in Isabelle/HOL” in the Chalmer’s Formal Methods group in Gothenburg, Sweden.
- September, T. Bourke participated in the Modelica conference in Versailles, France.
- October, T. Bourke participated in the Embedded Systems Week conferences in Amsterdam, The Netherlands.
- October, T. Bourke presented “Some recent improvements in modelling Loosely Time-Triggered Architectures” at the Journées Nationales GEOCAL-LAC-LTP 2015 in Nancy, France.
- November, T. Bourke presented “Zélus : un langage synchrone avec équations différentielles ordinaires” in the tool session of the 10th colloquium on the Modélisation des Systèmes Réactifs (MSR 2015) in Nancy, France.
- December, T. Bourke presented “Verification of code generation for a Lustre language” at the SYNCHRON workshop in Kiel, Germany.
- December, T. Bourke presented “Showing safety properties of a layered reactive model in Isabelle/HOL” at the University of Iowa, USA.
- December, T. Bourke presented “Towards the verified compilation of Lustre” at the University of Iowa, USA.
- October, M. Pouzet gave an invited talk at the EMSOFT’2015 conference, in Amsterdam “Building a Hybrid Systems Modeler from Synchronous Language Principles”.
- April, F. Zappa Nardelli gave a Keynote at the EuroLLVM international conference, London, UK.
- July, F. Zappa Nardelli gave a Keynote at the TAP international conference, L’Aquila, Italy.

9.1.5. Leadership within the scientific community

Marc Pouzet is responsible with Sandrine Blazy (Prof., Univ. Rennes) of the group LTP (Language, Types, Proof) of the French GDR (Groupe de Recherche) GPL (Genie de la Programmation) from the CNRS. Two one-day seminars are organised every year. In 2015, one seminar in Bordeaux; the second was 12-14 october 2015, in Nancy, and together with the groups LAC and GeoCal.

Albert Cohen is a member of the Steering Committee of the ACM PPoPP and Compiler Construction conferences.

Albert Cohen is a Steering Committee member of the HiPEAC 3 network of excellence.

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: “Operating Systems Principles and Programming” (M1), 38h, École Polytechnique, France

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

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

Licence : F. Zappa Nardelli: “Programmation Concurrente et Distribuée” (L3), TDs, 32h, École 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 : J. Vuillemin & 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 : Guillaume Baudart, 3rd year, supervised by T. Bourke and M. Pouzet

PhD in progress : Robin Morisset, 3rd year, supervised by F. Zappa Nardelli.

PhD in progress : Adrien Guatto, 4th year, supervised by A. Cohen and M. Pouzet, defended in January 2016.

PhD in progress : Riyadh Baghdadi, 4th year, supervised by A. Cohen and S. Verdoolaege, defended in September 2015.

PhD in progress : Nhat Minh Lê, 3rd year, supervised by A. Cohen.

PhD in progress : Ivan Llopard, 4th year, supervised by A. Cohen, defense in February 2016.

PhD in progress : Jie Zhao, 1st year, supervised by A. Cohen.

PhD in progress : Chandan Reddy, 1st year, supervised by A. Cohen.

M2 Internship: Virgile Andreani (Ecole normale supérieure, MPRI) supervised by T. Bourke and M. Pouzet.

L3 Internship: Chaitanya Malaviya (Nanyang Technological University) supervised by T. Bourke and M. Pouzet.

M1 Internship: Léo Testard (UPMC) - June/July 2015. Supervised by M. Pouzet

M1 Internship: Valentin Lorentz (Ecole normale supérieure de Lyon) - April/July 2015. Supervised by M. Pouzet

9.2.3. Juries

Albert Cohen was in the committees of

- Habilitation thesis, as reviewer: Marc Pérache (2015, U. Versailles and CEA DAM), Vincent Gramoli (2015, U. Pierre et Marie Curie et U. New South Wales, Australia);
- Habilitation thesis, as examiner: Dumitru Potop-Butucaru (2015, U. Pierre et Marie Curie and Inria), Stéphane Louise (2015, U. Versailles and CEA LIST);
- PhD thesis, as a reviewer: Diego Caballero (2015, U. Politècnica de Catalunya), Mohamed Bergach (2015, U. Nice Sophia-Antipolis), Lokesh Gidra (2015, U. Pierre et Marie Curie), Zakaria Bendifallah (2015, U. Versailles), Manuel Selva (2015, U. Lyon), Stefan Geuns (2015, U. Twente, The Netherlands), Jarryd Beck (2015, U. New South Wales, Australia), Jean-François Dollinger (2015, U. Strasbourg), Artem Shinkarov (2015, U. Heriot Watt, UK), Eugene Yip (2015, U. Auckland, New Zealand);
- PhD thesis, as an examiner:

Andi Drebes (2015, U. Pierre et Marie Curie),

Alexandre Aminot (2015, U. Grenoble).

Marc Pouzet was member of the PhD jury of Arlen Cox (2015, Univ. of Boulder).

Marc Pouzet was reviewer of the PhD thesis of Bernhard Thiele (2015, TUM, Munich)

Marc Pouzet was a member of the recruiting jury for two assistant professor positions at Chalmers University, Sueden, during spring 2015.

Marc Pouzet was a member of the recruiting jury for two Prof. position at University Paris Diderot, during spring 2015.

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 was general chair of the workshop “**Modélisation et représentation musicale**”, GDR ESARS, Bordeaux,

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

- D. Janin, PC Chair of **ACM Workshop on Functional Art, Music, Modeling and Design (FARM)**, Vancouver (Canada), associated with ICFP,

10.1.2.2. Member of the conference program committees

- M. Desainte-Catherine, PC member of **Journées d’Informatique Musicale (JIM 2015)**, Montréal (Canada),
- M. Desainte-Catherine, PC member of **Sound and Music Computing (SMC 2015)**, Maynooth (Ireland),
- M. Desainte-Catherine, PC member of **International Conference on Digital Audio Effects (DAFX 2015)**, Trondheim (Norway).

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)**, **Iranian Journal of Fuzzy Systems (IJFS)**, **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. Invited talks

- S. Salvati, LIF seminar, "Formal language theory and lambda-calculus", February 2015
- M. Desainte-Catherine, Albi Seminar *Les nouveaux territoires de la création*, "Jouer avec le temps", March 2015,
- S. Salvati, Choccola meeting, "Model construction for higher-order model-checking", April 2015
- S. Salvati was an invited speaker of the conference Finite State Methods in Natural Language Processing, "Context-freeness, automata and denotational semantics", June 2015
- S. Salvati, NII seminar "Model construction for higher-order model checking", July 2015,
- D. Janin, Dagstuhl Seminar *Verification of Evolving Graph Structures*, "Higher dimensional strings", November 2015,
- D. Janin, RNSC MuSICAL meeting, "Visualisation et programmation musicale via l'algèbre", December 2015,
- D. Janin, workshop GDR Esthétique Arts et Science (ESARS), "Représentation musicale et algèbre", Novembre 2015,
- M. Desainte-Catherine, colloque A& S FACTS, "Projet A& S le chant du filament", with Nicolas Villenave, November 2015,
- M. Desainte-Catherine and J.-M. Celerier, workshop GDR Esthétique Arts et Science (ESARS), "Structuration du temps avec i-score", Bordeaux, November 2015.

10.1.5. 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).

10.1.6. Scientific expertise

- Expertise of Art and Science projects of Diagonale Paris-Saclay.
- Expertise of projects for the young researcher award of Science and Music colloque at the University of Rennes.

10.1.7. 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

HdR : Sylvain Salvati, “Lambda-calculus and formal language theory”, Université de Bordeaux, defended in december 2015,

PhD : Jaime Arias, “Formal Semantics and Automatic Verification of Hierarchical Multimedia Scenarios with Interactive Choices”, Université de Bordeaux, defended in november 2015, supervised by M. Desainte-Catherine,

PhD : Jérôme Kirman, “Mise au point d'un formalisme syntaxique de haut niveau pour le traitement automatique des langues”, Université de Bordeaux, defended in december 2015, supervised by Bruno Courcelle, Lionel Clément, Sylvain Salvati,

PhD in progress : Pauline Mouawad, “Analyse et modélisation de l'émotion musicale”, started in september 2012, supervised by M. Desainte-Catherine,

PhD in progress : Etienne Dubourg, “Contribution à la théorie des langages de tuiles”, started in november 2012, supervised by D. Janin,

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

- M. Desainte-Catherine was a member and a reviewer of the PhD jury of Olivier Perrotin, “Chanter avec les mains : Interfaces chironomiques pour les instruments de musique numériques”, Université Paris-Saclay(LIMSI), Septembre 2015,

- M. Desainte-Catherine was a member and a reviewer of the PhD jury of Ko Yi Chun, “L’espace sensible : expérience inter-sensorielle et corporelle, à partir des dispositifs musicaux interactifs”, Université Vincennes Saint-Dennis, Novembre 2015,
- D. Janin was a member and the president of the PhD jury of Jaime Arias: “Formal Semantics and Automatic Verification of Hierarchical Multimedia Scenarios with Interactive Choices”, Université de Bordeaux (LaBRI), November 2015,
- S. Salvati was a member of the PhD jury of Yann Salmon: “Analyse d’atteignabilité pour les programmes fonctionnels avec stratégie d’évaluation en profondeur”, Université de Rennes 1, December 2015.

SPADES Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. General chair, scientific chair

- Alain Girault was general chair of the 10th International Federated Conference on Distributed Computing Techniques (DisCoTec'15), held in Grenoble in June 2015. <http://discotec2015.inria.fr>
- Jean-Bernard Stefani was the organization chair of the 7th Reversible Computation (RC'15) conference, held in Grenoble in July 2015. <http://www.reversible-computation.org/2015>

9.1.1.2. Member of the organizing committees

- Jean-Bernard Stefani was organiser chair for the 10th International Federated Conference on Distributed Computing Techniques (DisCoTec'15), held in Grenoble in June 2015. <http://discotec2015.inria.fr>
- Sophie Quinton was workshops chair for the 10th International Federated Conference on Distributed Computing Techniques (DisCoTec'15), held in Grenoble in June 2015. <http://discotec2015.inria.fr>

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- Alain Girault was technical program committee co-chair for the ACM/IEEE International Conference on Embedded Software (EMSOFT'15), held in Amsterdam in October 2015. <http://esweek.acm.org/esweek2015/emsoft>
- Jean-Bernard Stefani was program committee co-chair for the 5th Reversible Computation conference (RC'15), held in Grenoble in July 2015. <http://www.reversible-computation.org/2015>
- Sophie Quinton was co-chair of the 6th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS'15), held in Lund in July 2015. <http://waters2015.inria.fr>

9.1.2.2. Member of the 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'15), the Design Automation Conference (DAC'15), and the International Symposium on Industrial Embedded Systems (SIES'15).
- Gregor Gössler served in the program committee of the 10th International Federated Conference on Distributed Computing Techniques (FORTE'15).
- Sophie Quinton served in the program committees of the 27th Euromicro Conference on Real-Time Systems (ECRTS'15), the 20th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'15), the 2nd International Workshop on Multi-Objective Many-Core Design (MOMAC'15), and the 3rd International Workshop on Mixed Criticality Systems (WMC'15).
- Jean-Bernard Stefani served in the program committee of the 12th International Colloquium on Theoretical Aspects of Computing (ICTAC'15).

9.1.2.3. Reviewer

- Alain Girault reviewed an article for ECRTS'15.

- Gregor Gössler reviewed articles for ECRTS' 15
- Xavier Nicollin reviewed an article for DATE' 16.
- Sophie Quinton reviewed articles for DAC' 15, FORTE' 15, SIES' 15, DATE' 16.

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

- Pascal Fradet reviewed articles for LNCS Transactions on Aspect-Oriented Software Development.
- Alain Girault reviewed an article for the Journal on Advances in Signal Processing.
- Gregor Gössler reviewed articles for ACM Transactions on Embedded Computing Systems (TECS), Acta Informatica, and the EURASIP Journal on Embedded Systems.
- Sophie Quinton reviewed articles for the journal Real-time Systems and the Transactions on Design Automation of Electronic Systems,
- Jean-Bernard Stefani reviewed articles for Theoretical Computer Science.

9.1.4. Scientific expertise

- Alain Girault was reviewer for an ERC grant.

9.1.5. 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.
- Alain Girault was head of science (“Délégué scientifique”) of the INRIA Grenoble – Rhône-Alpes research center until June 2015.
- Alain Girault has been Vice Chair of the INRIA Evaluation Committee since September 2015. 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).
- Gregor Gössler has been leading a working group with the goal of fostering collaborations on the topic of formal methods for system design between the INRIA Grenoble – Rhône-Alpes research center and CEA Tech since September 2015.
- Jean-Bernard Stefani has been head of science of the INRIA Grenoble – Rhône-Alpes research center from July 2015. 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, 18 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Algorithmique et Structures de données 1, 22,5 HeqTD, niveau L3, Grenoble INP (Ensimag), France

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

Master : Jean-Bernard Stefani, Formal aspects of component software, 6h, MOSIG, Univ. Grenoble Alpes, France

9.2.2. Supervision

- PhD: Vagelis Bebelis, “Boolean Parametric Data Flow – Modeling – Analyses – Implementation”, Univ. Grenoble Alpes, defended on February 26th 2015, co-advised by Pascal Fradet and Alain Girault.
- PhD: Dmitry Burlyayev, “Design, Optimization, and Formal Verification of Circuit Fault-Tolerance Techniques”, Univ. Grenoble Alpes, defended on November 26th 2015, co-advised by Pascal Fradet and Alain Girault.
- PhD in progress: Yoann Geoffroy, “Towards a general causality analysis framework”, Univ. Grenoble Alpes, since October 2013, advised by Gregor Gössler.
- PhD in progress: Christophe Prévot, “Early Performance assessment for evolving and variable Cyber-Physical Systems”, Univ. Grenoble Alpes, since November 2015, advised by Alain Girault and Sophie Quinton.

9.2.3. Juries

- Alain Girault was member of the PhD jury of Paul-Antoine Arras (Univ. Bordeaux).
- Alain Girault was referee for the PhD of Julien Heulot (INSA Rennes).
- Jean-Bernard Stefani was president of the PhD jury of Jakub Zwolakowski (U. Paris-Diderot).
- Jean-Bernard Stefani was member of the HDR jury of Philippe Merle (U. Lille).
- Jean-Bernard Stefani was referee for the HDR of Luc Fabresse (U. Lille).
- Jean-Bernard Stefani was referee for the PhD of Vincent Lanore (ENS Lyon).
- Sophie Quinton was member of the jury for a “Maître de Conférences” position in Nancy.

9.3. Popularization

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

⁰<http://www.inria.fr/centre/grenoble/actualites/logiciel-embarque-et-responsabilite>

TEA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. Member of the organizing committees

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. Chair of conference program committees

Jean-Pierre Talpin co-chaired the AVICPS'15 workshop at RTSS'15

10.1.2.2. Member of the conference program committees

Jean-Pierre Talpin served the program committee of:

- MEMOCODE'15, 13th ACM-IEEE International Conference on Formal Methods and Models for System Design
- ACVI'15, 2nd Workshop Architecture Centric Virtual Integration
- AVICPS'15, 5th Analytic Virtual Integration of Cyber-Physical Systems Workshop
- FACS'15, 12th International Conference on Formal Aspects of Component Software
- FTSCS'15, 8th International Workshop on Formal Techniques for Safety-Critical Systems
- ICESS'15, 12th International Conference on Embedded Software and Systems
- SCOPES'15, 18th International Workshop on Software and Compilers for Embedded Systems
- SAC'15, 30th ACM/SIGAPP Symposium on Applied Computing

Thierry Gautier served as program committee member for the 2015 Electronic System Level Synthesis Conference, ESLsyn 2015 (<http://ecsi.org/eslsyn>).

10.1.2.3. reviewer

Thierry Gautier reviewed for ICCAD 2015 and MEMOCODE 2015.

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).

Jean-Pierre Talpin was Guest Editor of two special issues of the ACM TECS on *Architecture-Centric Virtual Integration* and on *Formal Methods for System Design*.

10.1.3.2. reviewer

Jean-Pierre Talpin reviewed articles for Acta Informatica.

Thierry Gautier reviewed for Frontiers of Computer Science.

10.1.4. Invited talks

Jean-Pierre Talpin gave a lecture on "Sémantique formelle de modèles d'architecture" at the Ecole temps-réel 2015 in Rennes

10.1.5. Scientific expertise

Jean-Pierre Talpin is co-author with Huafeng Yu and Sandeep Shukla of two patents filed with the USPTO:

- T1834.10134US01 – A timing-oriented and architecture-centric system design using contracts
- T1834.10131US01 – Bottom-up approach for integrating models for software components using contracts

10.2. Teaching - Supervision - Juries

10.2.1. Supervision

- Jean-Pierre Talpin is the supervisor of Simon Lunel's thesis on "*Timed contract algebras for correct by construction real-time system design*" and co-supervisor of Imré Frotier de la Mésselière with Mines ParisTech until June 2015.

10.2.2. Juries

Jean-Pierre Talpin served as Referee (rapporteur) for the HDR Thesis defense of Claire Paggetti , entitled "*Programmation sûre de plates-formes embarquées de type multi/pluri-cœurs*".

Jean-Pierre Talpin served as Referee (rapporteur) for the PhD. Thesis Defence of

- Elie Richa, Telecom ParisTech, entitled "*Qualification of Source Code Generators in the Avionics Domain : Automated Testing of Model Transformation Chains*".
- Ahlem Triki, Université de Grenoble , entitled "*Distributed Implementations of Timed Component-based Systems*".
- Yu Bai, TU Kaiserslautern , entitled "*Model-based Design of Embedded Systems by Desynchronization*".

ANTIQUÉ Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of steering committees

Jérôme Feret is member of the Steering Committee of the international Workshop on Static Analysis and Systems Biology (SASB). Xavier Rival is member of the Steering Committee of the international workshop on Tools for Automatic Program Analysis (TAPAS).

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committees

Xavier Rival is Co-Chair of the Program Committee of the Workshop on State Of the Art Program Analysis (SOAP'16), to be held in Santa Barbara (USA), June 2016. Xavier Rival is the Chair of the Program Committee of the 23rd Static Analysis Symposium (SAS'16), to be held in Edinburgh (UK), September 8–10, 2016.

8.1.2.2. Member of the conference program committees

Jérôme Feret was member of the Program Committee of the 2nd workshop on Verification of Engineered Molecular Devices and Programs (VEMDP'15), of the Program Committee of the 7th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO'15), of the Program Committee of the 6th International Workshop on Static Analysis and Systems Biology (SASB'15), of the Program Committee of the 25th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'15), and of the Program Committee of the 11th International Workshop on Developments in Computational Models (DCM'15). Jérôme Feret is a member of the Program Committee of the 8th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO'16), of the Program Committee of the 23rd Static Analysis Symposium (SAS'16), and of the Program Committee of the 14th International Conference on Computational Methods in Systems Biology (CMSB'16).

Xavier Rival was member of the Extended Review Committee (ERC) of the 41st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2015 PC), and of the Program Committee of the 13th Asian Programming Languages And Systems (APLAS'15), Pohang, Korea, November 30–December 2, 2015. Xavier Rival is a member of the Program Committee of the 1st International Conference on Functional Structures and Computational Deduction (FSCD'16), to be held in Porto, Portugal, June 2016, and of the Program Committee of the European Symposium On Programming (ESOP'17), 2017.

Cezara Drăgoi was a member of 15th International Conference on Application of Concurrency to System Design (ACSD'15), 41st International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'15), and 17th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNACS'15).

Vincent Danos was a member of the Program Committee of workshop on Integrative Cell Models, Lorentz Workshop, Leiden, and of the 7th Conference on Reversible Computation (RC'15), Grenoble.

8.1.2.3. Reviewer

Jérôme Feret was a reviewer for the 41st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2015), the 18th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'15), POPL 2015, the 27th International Conference on Computer Aided Verification (CAV'15), for the 26th International Conference on Concurrency Theory (CONCUR 2015), the International Conference on Embedded Software (EMSOFT'15).

Cezara Drăgoi was a reviewer for 27th International Conference on Computer Aided Verification (CAV'15), 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'16), and 30th Annual ACM/IEEE Symposium on Logic In Computer Science (LICS'15).

8.1.3. Journal

8.1.3.1. 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](#).

Vincent Danos is a member of the editorial board of [Mathematical Structures in Computer Science](#) journal (MSCS) and [Logical Methods in Computer Science](#) journal (LMCS).

8.1.3.2. Reviewer - Reviewing activities

Jérôme Feret was a reviewer for Information and Computation, Theoretical Computer Science, and Science of Computer Programming.

Xavier Rival was a reviewer for ACM TOPLAS (Transactions On Programming Languages and Systems).

8.1.4. Invited talks

Jérôme Feret was invited to give a talk on “the ANASTASEC project” at a joint meeting between Inria and CISCO, on “Model reduction of differential systems” at the working group “Model Reduction of Discrete models” (GDT BIOSS), at “La demi-heure de science” (Inria Paris-Rocquencourt), and at the Seminar of the Computer Science Department of the École normale supérieure, on “An algebraic approach for inferring and using symmetries in rule-based models” at the Seminar of the team PLUME (ENS Lyon).

Jérôme Feret was invited to give a speed talk on the ÁSTRÉE analyzer at the joint workshop between École normale supérieure and SAGEM, a speed talk on rule-based modeling in the international workshop on “Integrative Cell Models” (Leiden, Netherlands) and at the joint seminar between École normale supérieure and Pasteur Institute, and a speed talk on “An algebraic approach for inferring and using symmetries in rule-based models” at the first meeting of the Working group on Symbolic Systems Biology (GDT BIOSS).

Xavier Rival was invited to give a talk on “Modular design of static analyzers for program verification” at the KAIST Colloquium (KAIST, Daejeon, Korea), on May 4th, 2015.

Xavier Rival participated to the 56th Meeting of the IFIP Working Group 2.4 in Bopphard (Germany), and gave a talk on “Non contiguous array abstraction”.

Xavier Rival was invited to give a talk on “Construction of abstract domains for heterogeneous memory properties” in October 2015.

Cezara Drăgoi gave an invited talk on “PSync: A partially synchronous language for fault-tolerant distributed algorithms” at Dagstuhl Seminar 15191, “Compositional Verification Methods for Next-Generation Concurrency”, in May 2015, at LIAFA, University Paris 7 in the Verification seminar, and at the workshop on “The Chemistry of Concurrent and Distributed Programming II”, in June 2015.

Cezara Drăgoi gave an invited talk on “A Logic-based Framework for Verifying Consensus Algorithms” at Dagstuhl Seminar 15451 “Verification of Evolving Graph Structures”.

Cezara Drăgoi gave a tutorial on “Static analysis for data structures” at DACS in July 2015, and an invited talk at “La demi-heure de la science” on “Logic-based static analysis for the verification of programs with dynamically allocated data structures”.

Vincent Danos was invited to talk about “Computational Systems Biology” at Alan Turing Institute Scoping Workshop on networks, London, on Dec 14th, 2015.

Vincent Danos was invited to talk about “Design, optimization, and control in systems and synthetic biology” at Paris, ENS, on Nov 12th 2015.

Vincent Danos was invited to talk about “Models of growth” and the challenge of modelling processes which are embedded in a bigger adaptive system, keynote at the 16th International Workshop on Static Analysis and Systems Biology (SASB’15).

Vincent Danos was invited to talk about “Moment Semantics for Reversible Rule-Based Systems”, keynote at 7th Conference on Reversible Computation (RC’15), Grenoble.

8.1.5. Leadership within the scientific community

Xavier Rival is a member of the IFIP Working Group 2.4 on Software implementation technology.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence:

- Jérôme Feret, and Cezara Drăgoi, Mathematics, 40h, L1, FDV Bachelor program (Frontiers in Life Sciences (FdV)), Université Paris-Descartes, France.
- Antoine Miné and Xavier Rival, Semantics and applications to verification, 48h ETD, L3, École Normale Supérieure, Paris, France.
- Xavier Rival, Introduction to static analysis, 8h, L3, École des Mines de Paris, Paris, France.
- Xavier Rival, Introduction to algorithmics, 40h ETD, L3, École Polytechnique, Palaiseau, France.

Master:

- Vincent 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.
- Xavier Rival, Introduction to abstract interpretation, 8h, M1-M2, KAIST, Daejeon, Korea.
- Xavier Rival, Experimental Course on “Program Verification”, 20h ETD, M1, École Polytechnique, Palaiseau, France.
- Xavier Rival, Protocol safety and verification 20h ETD, M2 program in Advanced Communications and Network (École Polytechnique and Telecom Paris), France.
- Jérôme Feret has been invited to give a session (2h) in the Master M2IF (ÉNS Lyon) in the context of Russ Harmer’s course on Rule-based modelling.

8.2.2. Supervision

PhD:

- Arlen Cox, Parametric heap abstraction for dynamic languages libraries, École Normale Supérieure, 13th of April 2015, supervised jointly by Bor-Yuh Evan Chang (University of Colorado), Xavier Rival (Inria / École Normale Supérieure) and Sriram Sankaranarayanan (University of Colorado).
- Caterina Urban, Static analysis by abstract interpretation of functional temporal properties of programs, École Normale Supérieure, 29th of July 2015, supervised by Antoine Miné (CNRS / École Normale Supérieure) and Radhia Cousot (CNRS / École Normale Supérieure).
- Tie Cheng, Static analysis of spreadsheet applications, École Normale Supérieure, 23rd of September 2015, supervised by Xavier Rival (Inria / École Normale Supérieure).

PhD in progress:

- Mehdi Bouaziz, Static analysis of security properties by abstract interpretation, November 2011, Patrick Cousot and Jérôme Feret, École Normale Supérieure.
- Ferdinanda Camporesi, Abstraction of Quantitative Semantics of Rule-based models, January 2009, Radhia Cousot and Jérôme Feret (co-directed thesis with Maurizio Gabrielli, University of Bologna).
- Hugo Illous, Verification of memory properties by abstract interpretation, October 2015, Xavier Rival (co-directed thesis with Mathieu Lemerre, CEA Saclay).
- Huisong Li, Static Analysis of Data-Structures with Sharing, November 2014, Xavier Rival, École Normale Supérieure
- Jiangchao Liu, Verification of the memory safety of a micro-kernel, December 2013, Xavier Rival, École Normale Supérieure
- Antoine Toubhans, Combination of shape abstract domains, October 2011, Xavier Rival, École Doctorale de Paris Centre
- Thibault Suzanne, Thread-modular static analysis of concurrent programs in the presence of weak memory models, October 2014, Antoine Miné, École Normale Supérieure.
- Guillaume Terradot, "Modeles de croissance bacterienne/determinants de la taille", started in 2015, Vincent Danos, École Normale Supérieure.
- William Waites, "Strategie evolutionnaire dans des tissus avec interactions mecaniques" started in 2015, Vincent Danos, École Normale Supérieure.
- Andreea Beica, "Approximations max-paralleles de modeles stochastiques", started in 2015, Vincent Danos, École Normale Supérieure.

Internships:

- Eleonore Bellot did an internship at ENS with Vincent Danos on "Modeles energetiques de la cellule".
- Xavier Zaoui did an internship at ENS with Vincent Danos on "Croissance bacterienne et interferences entre antibiotiques".
- Danae David did an internship at ENS with Vincent Danos on "Representation des connaissances en biochimie des voies de signalisation".
- Ihab Boulas did an internship at ENS with Vincent Danos on "Modeles de transmission de plasmides "editeurs".

8.2.3. *Juries*

Jérôme Feret was reviewer of the PhD thesis of Peter Kreyßig (Friedrich-Schiller-Universität Jena, Germany, March 2015).

Jérôme Feret was examiner of the PhD thesis of Mounir Assaf (Irisa, France, May 2015).

Vincent Danos was referee on the phd thesis of Erwan Bigan, Universite Paris-Diderot, and referee on the phd thesis of Vincent Picard, Universite de Rennes 2.

8.2.4. *Selection committees*

Jérôme Feret was a member of the recruiting jury for junior research scientists (CR2) at Inria Paris-Rocquencourt in 2015; Jérôme Feret is a member of the recruitment committee for an assistant professor in Paris-Diderot University 2016.

CELTIQUE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

Static Analysis Symposium 2015, Saint-Malo, September 2015.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committees

SAS 2015 (Static Analysis Symposium) was chaired by Sandrine Blazy and Thomas Jensen

8.1.2.2. Member of the conference program committees

- FORTE 2015 (International Conference on Formal Techniques for Distributed Objects, Components and Systems): Alan Schmitt
- CoqPL 2016 (International Workshop on Coq for PL): Alan Schmitt
- POPL 2015 (Symposium on Principles of Programming Languages): David Pichardie (Program Committee) and Delphine Demange (External Review Committee)
- ESOP 2015 (European Symposium on Programming) : Delphine Demange
- JFLA 2015 (Journées Francophones des Langages Applicatifs) : Delphine Demange
- OCaml workshop 2015: Sandrine Blazy
- AFADL 2015 (Approches Formelles dans l'Assistance au Développement de Logiciels) : Sandrine Blazy
- ITP 2015 (Interactive Theorem Proving): Sandrine Blazy
- CPP 2016 (Certified Proofs and Programs): Sandrine Blazy
- IFIP SEC 2015: Thomas Jensen

8.1.2.3. Reviewer

- CONCUR 2015 (International Conference on Concurrency Theory): Alan Schmitt
- FOSSACS 2016 (International Conference on Foundations of Software Science and Computation Structures): Alan Schmitt
- ITP 2015 (International Conference on Interactive Theorem Proving) : Delphine Demange
- ATVA 2015 (13th International Symposium on Automated Technology for Verification and Analysis) : Sandrine Blazy
- ESOP 2015 (European Symposium on Programming): Thomas Jensen.

8.1.3. Journal

8.1.3.1. Reviewer - Reviewing activities

- Applied Mathematics & Information Sciences: Alan Schmitt
- Formal Aspects of Computing: Alan Schmitt, Thomas Jensen
- International Journal of Computer Mathematics: Alan Schmitt
- Journal of Automated Reasoning: Sandrine Blazy, David Pichardie
- Journal of Computer Security : Sandrine Blazy

8.1.4. Invited talks

- Sandrine Blazy: Formal verification of compilers and static analyzers, PLMW@POPL 2015 (Programming Languages Mentoring Workshop)
- Thomas Jensen: Integrating formal verification within programming languages. Seminar Collège de France, October 2015.

8.1.5. Scientific expertise

- Sandrine Blazy: expertise of 2 projects for FNR (Luxemburg)
- Thomas Jensen, expertise of ANR AAP general, short proposals

8.1.6. Research administration

- Thomas Jensen is head of the NUMERIC department at University of Bretagne-Loire
- Thomas Jensen is managing the “Security” track of ANR Comin Labs.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence: Thomas Genet, Software Engineering, 58h, L2, Université de Rennes 1 / Istic, France
 Licence: Delphine Demange, Software Engineering, 40h, L2, Université de Rennes 1 / Istic, France
 Licence: Delphine Demange, Functional Programming, 70h, L1, Université de Rennes 1 / Istic, France
 Licence : Alan Schmitt, Programmation Fonctionnelle, 39h, L3, Insa Rennes, France
 Licence : David Pichardie, Algorithms, 36h, L3, ENS Rennes, France
 Licence : David Cachera, Logic, 36h, L3, ENS Rennes, France
 Licence : Sandrine Blazy, Functional programming, 30h, L3, 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 Cachera, Semantics of Programming Languages, 36h, M1, Université Rennes 1, France
 Master : Frédéric Besson, Compilation, 50h, M1, Insa Rennes, France
 Master : Sandrine Blazy, Méthodes Formelles pour le développement de logiciels sûrs, 53h, M1, Rennes 1, France
 Master : Alan Schmitt, Méthodes Formelles pour le développement de logiciels sûrs, 25h, M1, Rennes 1, 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, Software vulnerabilities, 38h, M2, Université Rennes 1, France
 Master : Delphine Demange, Software Security, 9h, M2, Université Rennes 1, France
 Master : Thomas Jensen, Program Analysis and Software Security, 39h, M2, Université Rennes 1, France

8.2.2. Supervision

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

PhD in progress : Gurvan Cabon, Analyse non locale certifiée en JavaScript grâce à une sémantique annotée, 1st september 2015, Alan Schmitt

PhD in progress : Yon Fernandez De Retana, Verified Optimising Compiler for high-level languages, 1st september 2015, Delphine Demange and David Pichardie

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

PhD in progress : Florent Sadel, Vulnerability discovery, November 2015, Sandrine Blazy, Frédéric Besson and Frédéric Guihéry (Amossys)

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: Pierre Wilke, Low-level memory models for compilers and static analysers, 1st august 2013, Sandrine Blazy and Frédéric Besson

PhD in progress: Oana Andreescu, Static analysis and automated program proving, 1st September 2013, Thomas Jensen

PhD in progress: Pauline Bolignano, Modeling and abstraction of system software, 1st November 2013, Thomas Jensen

PhD: Yann Salmon, Reachability for Term Rewriting Systems under Strategies, defended Dec 2015, Thomas Genet

PhD: Vincent Laporte, Verified static analyses for low-level languages, defended Nov 2015, Sandrine Blazy and David Pichardie

PhD: Stéphanie Riaud, Data obfuscation for protecting programs against dynamic analysis, defended Dec 2015, Sandrine Blazy

8.2.3. *Juries*

Alan Schmitt, jury member (reviewer) for the PhD defense of Burak Ekici, December 2015, Université Grenoble Alpes

David Pichardie, jury member (chair) for the PhD defense of Mounir Assaf, May 2015, University Rennes 1, France.

David Pichardie, jury member (reviewer) for the PhD defense of Bogdan Mihaila, January 2015, Technische Universität München, Germany.

Sandrine Blazy, jury member for the PhD defense of Alexis Fouilhé, October 2015, Grenoble University, France

Sandrine Blazy, jury member for the PhD defense of Zakaria Chihani, November 2015, Ecole Polytechnique, France.

Sandrine Blazy, jury member for the PhD defense of Lourdes del Carmen Gonzalez Huesca, November 2015, Paris Diderot University, France.

Thomas Jensen, jury member for the PhD defense of Magnus Madsen, May 2015, Aarhus University, Denmark.

Thomas Jensen, jury member for the PhD defense of Clémentine Maurice, EURECOM, France.

Alan Schmitt, jury member for the selection of Inria CR (researcher) candidates, March and April 2015, Inria, Rennes, France.

Delphine Demange, jury member for the selection of a Maître de Conférences at University Paris Diderot (Paris 7) / LIAFA+PPS, May 2015, Paris, France.

Sandrine Blazy, jury member for the selection of a Maître de Conférences at University of Nancy, May 2015, Nancy, France.

Sandrine Blazy, jury member for the selection of a Maître de Conférences at University of Rennes 1, May 2015, Rennes, France.

Sandrine Blazy, jury member for the selection of a professor at University of Brest, May 2015, Brest, France.

Delphine Demange, jury member of the Gilles Kahn PhD award committee, December 2015, Inria Paris - Rocquencourt

8.3. Popularization

- IRISA 40th anniversary Open House - Recreational workshop (interactive demonstration) on the problem of functional correctness of programs, its importance in the field of critical software, and formal proof of correctness : Thomas Genet, Delphine Demange, Pauline Bolignano, Yannick Zakowski. Inria Convention centre, Inria Rennes - Bretagne Atlantique. Rennes, France. December 2015.
- Talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.”, Thomas Genet, given two times in high schools close to Rennes.
- Two short tutorials. One for Isabelle/HOL [41] and one for SPAN+AVISPA [42].

DEDUCTEAM Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events selection

9.1.1.1. Chair of conference program committees

Gilles Dowek was PC chair of TLCA-RTA.

9.1.1.2. Member of the conference program committees

Gilles Dowek was PC member of CADE, ICTAC and eMoocs.

Guillaume Burel was PC member of PxTP'15 and IWIL'15.

9.1.1.3. Reviewer

Frédéric Blanqui has reviewed papers for TYPES'14 post-proceedings and LICS'15.

Guillaume Burel has reviewed a paper for Tableaux'15.

Olivier Hermant has reviewed papers for Tableaux'15 and CADE-25, a project for ANR (second phase) and pre-projects for ANR (first phase).

9.1.2. Journal

9.1.2.1. Member of the editorial boards

Gilles Dowek is an editor of TCS.

9.1.2.2. Reviewer - Reviewing activities

Frédéric Blanqui reviewed a paper for TCS.

Guillaume Burek reviewed a paper for Formal Aspects of Computing.

Olivier Hermant reviewed a paper for TCS.

9.1.3. Invited talks

Gilles Dowek was invited to DCM and Tools for teaching logic.

9.1.4. Scientific expertise

Gilles Dowek has been a consultant for the Conseil Scientifique des Programmes.

Gilles Dowek is the President of the Scientific board of the Société Informatique de France.

Gilles Dowek is a member of the Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistène (CERNA).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: Pierre Halmagrand, Initiation à la Méthode B, 54 HETD, M2, CNAM.

License: Frédéric Gilbert, Les principes des langages de programmation, 40, L3, Ecole Polytechnique.

License: Raphaël Cauderlier, Introduction aux Bases de Données Relationnelles, 21, L2, UPMC.

License: Raphaël Cauderlier, Projet (Application) : Android, 42, L2, UPMC.

License: Raphaël Cauderlier, Eléments de programmation 1, 58, L1, UPMC.

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

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

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

Master: Guillaume Burel, Systèmes et langages formels, 8.75 HETD, M1, ENSIIE.

Master: Guillaume Burel, Compilation, 24.5 HETD, M1, ENSIIE.

Master: Guillaume Burel, Preuve, Analyse statique, Vérification run-time, 13 HETD, M2 CILS, Paris-Saclay.

Licence: Guillaume Burel is in charge of the 4th and 5th semesters of the engineering degree at ENSIIE, and was responsible for the final engineer internship until September, 2015.

Gilles Dowek has given a course at the MPRI.

Gilles Dowek has been teaching at ENS-Cachan.

Gilles Dowek has given various talks about teaching informatics in primary and secondary education.

Gilles Dowek has participated to several training sessions for high school teachers with La Main à la Pâte.

Licence: Olivier Hermant, Introduction to Programming in Python, 100 HETD, L1-L3, Wesleyan University, USA.

9.2.2. Supervision

PhD: Simon Cruanes, Extending Superposition with Integer Arithmetic, Structural Induction, and Beyond [13], defended at École polytechnique on September the 10th, supervised by Guillaume Burel and Gilles Dowek.

PhD: Bruno Bernardo, An implicit Calculus of Constructions with dependent sums and decidable type inference [12], defended at École polytechnique on September the 18th, supervised by Bruno Barras and Gilles Dowek.

PhD: Ali Assaf, A framework for defining computational higher-order logics [11], defended at École polytechnique on September 28, 2015, supervised by Gilles Dowek and Guillaume Burel.

PhD: Kailiang Ji, Model Checking and Theorem Proving [14], defended at Paris Diderot on September 25, 2015, supervised by Gilles Dowek.

PhD: Ronan Saillard, Typechecking in the $\lambda\Pi$ -Calculus Modulo: Theory and Practice [55], defended at MINES ParisTech on September 25, 2015, supervised by Olivier Hermant and Pierre Jouvelot.

PhD in progress: Guillaume Bury, Deduction Modulo Theory, started October 1st, 2015, supervised by David Delahaye and Gilles Dowek.

PhD in progress: Raphaël Cauderlier, Object-oriented mechanisms for interoperability of proof systems, started September 1st, 2013, supervised by Catherine Dubois.

9.2.3. Juries

Gilles Dowek is a member of the prix Le Monde de la Recherche Universitaire.

9.3. Popularization

Gilles Dowek has given various popular science talks.

Gilles Dowek writes a monthly chronicle in Pour la Science.

Gilles Dowek is a member of the Scientific board of La Main à la Pâte.

ESTASYS Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events selection

- Axel Legay was PC member of MEMOCODE, FORMATS, FORMALIZE, SPLC, ASE, FACS, FORTE.
- Louis-Marie Traonouez was PC member of FORMATS
- Rudolf Fahrenberg was PC member of TACAS

8.1.2. Journal

8.1.2.1. Member of the editorial boards

Axel Legay is a member of the editorial board of the newly created journal for masterminding changes (FOMACS).

8.1.2.2. Reviewer - Reviewing activities

Axel Legay has been reviewer for TCS, FMSD, IandC.

8.1.3. Invited talks

- Axel Legay has been invited at the first EMSIG school, Copenhagen 2015.
- Uli Fahrenberg has been invited at Automatha 2015.

8.1.4. Leadership within the scientific community

Together with the University of Vannes and IRIT Toulouse, the team has initiated the first GT on systems of systems.

8.1.5. Scientific expertise

Axel Legay has been an evaluator for the National Science fund in Belgium. He is also a member of Inria evaluation committee.

8.1.6. Research administration

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Software Verification

Axel Legay: Software Verification, 40 hours, Royal Holloway, University of London

Axel Legay: Modélisation et Vérification Formelle par Automates, 12 hours, University of Rennes 1.

Axel Legay: Méthodes d'analyse de risques, 28 hours, ENSIBS2 (Vannes)

Jean Quilbeuf: Modélisation et Vérification Formelle par Automates, TP 12 hours, University of Rennes 1.

8.2.2. Supervision

PhD: Mounir Chadli: Scheduling for Systems of Systems, Started on December 2014, Axel Legay

[1] HdR: Axel Legay, Contribution to Statistical Model Checking, November 2015

8.2.3. Juries

Axel Legay has been a member of the PhD jury of Raphael Michel (Namur).

8.3. Popularization

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

GALLIUM Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. Member of organizing committees

Didier Rémy is a member of the steering committees of the OCaml workshop and the ML Family workshop.

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

Arthur Charguéraud served as program committee chair for for the second International Workshop on Coq for Programming Languages (CoqPL 2016).

Damien Doligez served as program committee chair for the OCaml Users and Developers workshop (OUD 2015).

10.1.2.2. Member of conference program committees

Umut Acar was a member of the program committees of the 30th IEEE International Parallel and Distributed Processing Symposium (IPDPS 2016) and of the workshop on Algorithms and Systems for MapReduce and Beyond (BeyondMR 2016). He was also a member of the External Review Committee of the 43rd ACM Symposium on Principles of Programming Languages (POPL 2016).

Xavier Leroy was a member of the program committees of the 1st Summit on Advances in Programming Languages (SNAPL 2015) and of the Compiler Construction conference (CC 2016).

Xavier Leroy was a member of the award committee for the 2015 ACM SIGPLAN Software System award.

Mike Rainey was a member of the program committee of the International Conference on Functional Programming (ICFP 2015).

Arthur Charguéraud and Didier Rémy were members of the program committee of the European Symposium on Programming Languages (ESOP 2016).

10.1.2.3. Reviewer

In 2015, the members of Gallium reviewed at least 80 conference submissions.

10.1.3. Journal

10.1.3.1. Member of 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 a member of the editorial board of the Journal of Functional Programming.

10.1.3.2. Reviewer

In 2015, the members of Gallium reviewed at least 4 journal submissions and 10 grant proposals.

10.1.4. Leadership within the scientific community

Pierre Courtieu and Xavier Leroy are members of the Coq steering committee.

10.1.5. Research administration

Xavier Leroy is *délégué scientifique adjoint* of Inria Paris-Rocquencourt and an appointed member of Inria's *Commission d'Évaluation*. In 2015, he participated in the following Inria hiring and promotion committees: *jury d'admissibilité CR2 Paris-Rocquencourt* (vice-chair); *jury d'admissibilité CR2 Nancy*; and *promotions CRI*. He was a member of the hiring committee for a professor position at ENS Rennes.

Luc Maranget is an elected member of the *Comité Technique Inria*.

Luc Maranget chairs the *Commission des utilisateurs des moyens informatiques – Recherche* of Inria Paris-Rocquencourt.

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 represents Inria in the *commission des études* of the MPRI master, co-organized by U. Paris Diderot, ENS Cachan, ENS Paris, and École Polytechnique.

Didier Rémy is Inria's *Deputy Scientific Director* (ADS) in charge of *Algorithmics, Programming, Software and Architecture*.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Xavier Leroy and Didier Rémy, “Functional programming languages”, 45h, 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.

Licence: François Pottier, “Programmation avancée” (INF441), 20h, L3, École Polytechnique, France.

Master: François Pottier, “Compilation” (INF564), 20h, M1, École Polytechnique, France.

Master: François Pottier, “Programming with permissions in Mezzo”, 4.5h, M2, 15th SFM summer school, Bertinoro, Italy.

Licence: Mike 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.

10.2.2. Supervision

M2 (Master Pro): Keryan Didier, Université Denis Diderot, supervised by Luc Maranget.

M2 (MPRI): Benjamin Farinier, Université Paris Diderot, supervised by François Pottier.

M2 (MPRI): Armaël Guéneau, ENS Lyon, supervised by Arthur Charguéraud and François Pottier.

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: Jacques-Henri Jourdan, “Verasco: a formally verified C static analyzer”, Université Paris Diderot, since September 2012, supervised by Xavier Leroy.

PhD in progress: Gabriel Scherer, “Which types have a unique inhabitant?”, Université Paris Diderot, since October 2011, supervised by Didier Rémy.

PhD in progress: Thomas Williams, “Putting Ornaments into practice”, Université Paris Diderot, since September 2014, supervised by Didier Rémy.

10.2.3. Juries

Pierre Courtieu was a member of the Ph.D. jury of Sylvain Dailier, Université d'Orléans, December 2015.

Xavier Leroy was a member of the PhD juries of Tie Cheng, ENS Paris, September 2015; Vincent Laporte, Université Rennes 1, November 2015; and Robbert Krebbers, Radboud University, December 2015.

François Pottier was president of the Ph.D. jury of Bruno Bernardo, École Polytechnique, September 2015.

10.3. Popularization

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

Jacques-Henri Jourdan and Fabrice Le Fessant manned a stand at “Salon Culture & Jeux Mathématiques” in Paris.

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

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

Since 2012, the Gallium team has published a research blog at <http://gallium.inria.fr/blog/>, edited by Gabriel Scherer. This blog continued its activity in 2015, with 10 posts from 8 different authors.

MARELLE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

Yves Bertot is member of the organizing committee for the UITP (User-Interfaces for Theorem Provers) series of workshops.

Enrico Tassi organized a Coq coding Sprint in Sophia Antipolis, June 22-25, in Sophia Antipolis. There were 39 attendants.

Yves Bertot organized a Coq workshop in Sophia Antipolis on June 26. There were around 40 attendants.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

Yves Bertot was a member of the conference program committee for ITP'15 (Interactive Theorem Proving).

Cyril Cohen was a member of the conference program committee for JFLA'16 (Journées Francophones des Langages Applicatifs).

Laurent Théry was a member of the program committee for PxTP'15 (Proof exchange for Theorem Provers).

9.1.2.2. Reviewer

Members of the project reviewed papers for the conferences CPP'16 (Certified Programs and Proofs), ESOP'15 (European Symposium on Programming), Types, LICS'15 (Logic in Computer Science), Cade'15 (Conference on Automated Deduction), ITP'15 (Interactive Theorem Proving), JFLA'16 (Journées Francophones des langages applicatifs).

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

Members of the project-team reviewed papers for the journals *Journal of Functional Programming*, *Journal of Formal Reasoning*, *Journal of Automated Reasoning*.

9.1.4. Invited talks

Laurence Rideau gave an invited talk at the conference TFP'15 (Trends in Functional Programming).

Cyril Cohen and Yves Bertot gave invited talks at the workshop on Algebra, Geometry, and Proofs in Symbolic Computation in Toronto in December.

Cyril Cohen and Enrico Tassi gave lectures at the tutorial on Coq organized as satellite event to ITP'15 in Nanjing, China, in August.

9.1.5. Research administration

- Members of the project-team evaluated project for the French national agency for research funding (ANR).
- José Grimm is a member of the local committee for Hygiene and Work Safety.
- Cyril Cohen regularly serves as secretary for the local committee of project-team leaders.
- Yves Bertot is the chairman of the *Coq Steering committee*, Enrico Tassi is a member of this committee.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Laurence Rideau, "programming and algorithms", 50 hours, Lycée Masséna, Nice, France.

Licence : Cyril Cohen, "paradigms of programming languages", 12 hours, University of Nice, France.

Master : Yves Bertot and Enrico Tassi, "software verification and computer proof", 21 hours, Université de Nice, France.

Master : Laurent Théry, "introduction to Coq", 3 hours, Ecole des Mines de Paris, France.

9.2.2. Supervision

PhD in progress : Boris Djalal, starting in October 2015, supervised by Yves Bertot and Cyril Cohen

9.2.3. Juries

Yves Bertot was examiner with written report duty for the thesis of Catherine Lelay (University of Paris-south) and examiner for the thesis of Robbert Krebbers (Radboud University Nijmegen).

MEXICO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. 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 <http://projects.lsv.ens-cachan.fr/informel/>. Among many other activities, the LIA organised another edition of the ACTS workshop, see [here](#).

The renewal beyond 2015 has been approved by CNRS' national committee, the FSD's approval is pending.

10.1.2. Scientific events organisation

10.1.2.1. General chair, scientific chair

Serge Haddad is a member of the steering committee for ICATPN.

10.1.3. Scientific events selection

10.1.3.1. Chair of conference program committees

- Stefan Haar was co-chair of the program committee of the conference Application of Concurrency to System Design (ACSD) 2015 [38].

10.1.3.2. Member of the conference program committees

- Thomas Chatain was a member of the program committee of the conference Application of Concurrency to System Design (ACSD) 2015 [38].
- Paul Gastin was a member of the program committee of the workshop ACTS 2015.
- Stefan Haar was a member of the program committees of the ETFA 2015 workshop, the CHIA 2015 workshop, and of the SAFEPROCESS 2015 Symposium and the ICTAC 2015 conference.
- Stefan Schwoon was a member of the PCs for ICATPN 2015 and SPIN 2015.
- Serge Haddad was a member of the PCs of the workshops
 - FOR-MOVES, associated with ICSOC 2015, Goa, India;
 - VECOS 2015, Bejaia, Algeria;
 - ADECS and PNSE, both associated with ICATPN 2015, Brussels, Belgium.

10.1.3.3. Reviewer

- Stefan Haar was a reviewer for CSL 2015, ACC 2015
- Stefan Schwoon was a reviewer for the 2015 editions of SODA, TAMC, POPL, and TACAS.
- Paul Gastin, Benedikt Bollig and Serge Haddad are regularly reviewers for many international conferences.

10.1.4. Journal

10.1.4.1. Member of the editorial boards

- Paul Gastin is on the advisory boards of *Journal of Automata, Languages and Combinatorics* and of the EATCS Springer Book series *Monographs in Theoretical Computer Science* and *Texts in Theoretical Computer Science*.
- Serge Haddad was Editor of one edition of the TOPNOC journal (LNCS 8910).
- Stefan Haar is an associate editor for the *Journal of Discrete Event Dynamic systems*.

10.1.4.2. Reviewer - Reviewing activities

- Stefan Haar was a reviewer for *Automatica*, *Journal of Computer and System Sciences*, *IEEE Transactions on Automatic Control*, *Computer Journal* and *TOPNOC*. He is also a regular reviewer for *AMS Mathematical Reviews*.
- Thomas Chatain was a reviewer for reviewer for *ACM Transactions on Embedded Computing Systems*.
- Stefan Schwoon acted as reviewer for the journals TCS, Fundamenta, STTT, FAOC (Formal Aspects of Computing), and ToPNoC.
- Paul Gastin, Benedikt Bollig and Serge Haddad are regularly reviewers for many international journals.

10.1.5. Invited talks

- Serge Haddad gave invited talks
 - on 'Active Diagnosis', July 7, 2015, Turin University;
 - on 'Time and Stochastic Petri Nets', June 22, during the Petri Nets tutorials at ICATPN 2015, Brussels, Belgium;
 - on 'Polynomial Interrupt Timed Automata' at Inria Rennes, Sept. 17,
 - on 'probabilistic automata' at *Ecole Jeunes Chercheurs EJCIM 2015*, April 1st, 2015, Orléans, France.
- Paul Gastin was an invited speaker for
 - 'Formal methods for the verification of distributed algorithms' Invited talk at **INFINITY 2015**, Bangalore (India), December 15, 2015.
 - 'Weighted Automata: Highlighted Excerpts.' Tutorial at **HIGHLIGHTS'15**, Prague, September 15, 2015.
 - Gossip: Maintening latest information beyond channel bounds.
 Invited talk at **ALFA'15**, Bordeaux (France), June 15 - 17, 2015, and talk at **FRIDA'15**, Grenoble (France,) June 5, 2015.
 - '10 years of weighted logics for weighted automata.' Invited talk at **AutoMathA**, Leipzig (Germany), May 6 - 9, 2015.
- Benedikt Bollig was an invited speaker
 - at the 22nd International Symposium on Temporal Representation and Reasoning (TIME 2015), Kassel, Germany
 - at the 20th International Conference on Implementation and Application of Automata (CIAA 2015), Umeå, Sweden
 - at the 2nd Workshop on Parameterized Verification, Madrid, Spain
 - at ALFA 15: Automata, Logic, Formal languages, Algebra, Bordeaux, France
 - at Automata, Concurrency and Timed Systems (ACTS 2015), Chennai, India
- Stefan Schwoon gave a talk in the CASSTING workshop in Brussels on May 18th, 2015.

10.1.6. Scientific expertise

- Serge Haddad was member of a selection committee for a professor's position at U. Paris 6, and an external expert for the evaluation of ONERA's DCPS department in November 2015.

10.1.7. Research administration

- Paul Gastin is director of the LIA **INFORMEL**.
- Stefan Haar is the Saclay Inria center's correspondent for european partnerships. He also was a member of DIGITEO's project selection committee, and will be directing the *SCILEX* axis of the *LABEXDIGICOSME*.

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Note: We only list here the teaching activities of researchers, not the courses of full-time teachers in the team.

Licence : Stefan Haar, *Théorie des Langages*, 22.3 h (EQTD) L2, Université Paris-René Descartes, France

Master : Benedikt Bollig, *Non-Sequential Theory of Distributed Systems*, 22.5 h (EQTD), M2, Parisian Master of Research in Computer Science (MPRI), France

We further note that as of September 2015, Serge Haddad is no longer the coordinator of the M1 level but has become the director of the computer science department of ENS Cachan, as the successor of Paul Gastin in this position; and Stefan Schwoon has become the coordinator of the L3 level.

10.2.2. Supervision

- PhD in progress :
 - Engel Lefauchaux, *controlling information in probabilistic systems*, Co-supervisors Serge Haddad and Nathalie Bertrand (Inria Rennes, SUMO team);
 - Yann Duploux, *application of formal methods to the development of embedded systems for autonomous vehicles*, since Sept. 2015, Supervisor Serge Haddad (with Béatrice Berard, UPMC).
 - Simon Theissing, *Supervision for Multi-Modal Transport Systems*, since September 2013, Supervisor Stefan Haar
 - Salim Perchy (Ecole Polytechnique), *D-spaces*, since November 2013, co-supervisor Stefan Haar, Supervisor Franck Valencia (Note : S. Perchy belongs to the COMETE team, not MEXICO).

10.2.3. Juries

- Benedikt Bollig was a member of the PhD committee of Mathieu Caralp, "Problèmes de bornes pour les automates et les transducteurs à pile visible", December 18, 2015 at Université Marseille.
- Paul Gastin was
 - President of the PhD committee for Jad Hamza at University Paris-Diderot, on November 27, 2015;
 - Reviewer for the theses of Roy Mennicke, Universität Ilmenau (Germany), and of Vitaly Perevoshchikov, Universität Leipzig (Germany);
 - a member of the HdR committees of Nathalie Bertrand, Rennes, November 16 and of Benedikt Bollig, ENS Cachan, June 2, 2015;
 - reviewer of the HDR of Olivier Serre, University Paris-Diderot, March 10, 2015

- Serge Haddad was a member of the PhD committees of M. Amziani at Telecom SudParis in June 2015, and of D. Paquereau at INSA Lyon in March 2015.
- On May 27, 2015, *Thomas Chatain* was a member of the jury in the competition for recruitment of Master's level students at ENS Rennes.
- *Stefan Haar* was a reviewer of the thesis by Kari Kähkönen on *Automated Systematic Testing Methods for Multithreaded Programs*, defended on February 2, 2015, at Aalto University, Finland.
- *Stefan Haar* was a member of the PhD examination board of the Thesis of Houssame-Eddine Gougam on *Analyse de l'impact du temps sur la diagnosticabilité des systèmes à événements discrets*, defended on Sep 28, INSA Toulouse.

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

L. Straßburger was on the Organization Committee for the International Workshop on Efficient and Natural Proof Systems, held at the University of Bath 14-16 December, 2015

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

K. Chaudhuri was the Program Committee chair of the following meeting.

LFMTP 2015: Logical Frameworks and Meta-Languages: Theory and Practice
Co-chaired with Iliano Cervesato, Carnegie Mellon University (Qatar)

9.1.2.2. Member of conference program committees

D. Miller was on the Program Committees of the following meetings.

TABLEAUX 2015: Automated Reasoning with Analytic Tableaux and Related Methods, Wroclaw, Poland, September.

PPDP 2015: 17th International Symposium on Principles and Practice of Declarative Programming, Siena, Italy, 13-16 July.

PxTP 2015: Fourth Workshop on Proof eXchange for Theorem Proving, Berlin, Germany, 2-3 August.

ICALP 2015 (42nd International Colloquium on Automata, Languages, and Programming), Track B, Kyoto, Japan, 6-10 July.

S. Graham-Lengrand was on the Program Committees of the following meetings.

TABLEAUX 2015: Automated Reasoning with Analytic Tableaux and Related Methods, Wroclaw, Poland, September.

CSL 2015: 24th EACSL Annual Conference on Computer Science Logic, Berlin, Germany, 7-10 September.

K. Chaudhuri was on the Program Committees of the following meetings.

CPP 2015: ACM-SIGPLAN Conference on Certified Programs and Proofs

FICS 2015: International Workshop on Fixed Points in Computer Science

WoF 2015: International Workshop on Focusing

L. Straßburger was on the Program Committees of the following meetings.

FoSSaCS 2015: 18th International Conference on Foundations of Software Science and Computation Structures

WENSP: International Workshop on Efficient and Natural Proof Systems

G. Reis was on the Program Committee for the following meeting.

LFMTP 2015: Logical Frameworks and Meta-Languages: Theory and Practice

9.1.2.3. Reviewer

T. Libal was a reviewer for the following workshops:

Fourth Workshop on Proof eXchange for Theorem Proving.

S. Graham-Lengrand was a reviewer for the following conferences:

LPAR 2015: 20th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Suva, Fiji, November.

LICS 2015: 30th Annual ACM/IEEE Symposium on Logic in Computer Science, Kyoto, Japan, July.

D. Ilik was a reviewer for the following conferences:

ESOP 2015: 24th European Joint Conferences on Theory and Practice of Software

FoSSaCS 2015: 18th International Conference on Foundations of Software Science and Computation Structures

TLCA 2015: 13th International Conference on Typed Lambda Calculi and Applications

M. Volpe was a reviewer for the following conferences:

Tableaux 2015: 24th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods, Wroclaw, Poland, September.

L. Straßburger was a reviewer for the following conferences:

TLCA 2015: 13th International Conference on Typed Lambda Calculi and Applications

LPAR 2015: 20th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, Suva, Fiji, November.

FLOPS 2016: Thirteenth International Symposium on Functional and Logic Programming March 4-6, 2016, Kochi, Japan

B. Accattoli was a reviewer for the following conferences:

- CSL 2015: 24th EACSL Annual Conference on Computer Science Logic, Berlin, Germany, 7-10 September.
- TGC 2015: 10th International Symposium on Trustworthy Global Computing, Madrid, Spain, August 31 to September 1.
- FoSSaCS 2016: 19th International Conference on Foundations of Software Science and Computation Structures, to be held in Eindhoven, The Netherlands, 2-8 April 2016.

T. Brock-Nannestad was a reviewer for the following conferences:

- ITP 2015: 6th Conference on Interactive Theorem Proving, Nanjing, China, August 24–27 August, 2015.
- CPP 2016: The 5th ACM SIGPLAN Conference on Certified Programs and Proofs, Saint Petersburg, Florida, USA, January 18–19, 2016.

9.1.3. Journal

9.1.3.1. Editor-in-chief

D. Miller was Editor-in-Chief of the ACM Transactions on Computational Logic. He completed a six year term on June 2015.

9.1.3.2. 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).

D. Miller served on as an editor for Logical Methods in Computer Science for the production of a special issue for papers from CSL-LICS 2014.

K. Chaudhuri served as a guest editor for Mathematical Structures in Computer Science special issue on Logical Frameworks and Meta Languages, based on selected papers from LFMTTP 2015

9.1.3.3. Reviewer - Reviewing activities

- T. Libal was a reviewer for the following journals:
Journal of Automated Reasoning (Springer).
- S. Graham-Lengrand was a reviewer for the following journals: J. Appl. Logic, Theoret. Comput. Sci., Acta Inform.
- D. Ilik was a reviewer for the following journals:
Mathematical Reviews (MathSciNet)
Zentralblatt MATH
- M. Volpe was a reviewer for the following journals:
Annals of Mathematics and Artificial Intelligence;
Journal of Automated Reasoning;
Logica Universalis.
- L. Straßburger was a reviewer for the following journals:
Logical Methods in Computer Science (two articles)
Theoretical Computer Science, Elsevier
Ontos Mathematical Logic, Walter De Gruyter
Logic Journal of the IGLP, Oxford University Press
- B. Accattoli was a reviewer for the following journals:
 - Logical Methods in Computer Science (two articles)
 - Theoretical Computer Science, Elsevier

9.1.4. Invited talks

D. Miller was a plenary speaker at the joint meeting of LOPSTR 2015 and PPDP 2015 (Siena, Italy) and was an invited speaker at LSFA 2015 (Natal Brazil) and in the Session on History and Philosophy of Computing at the 15th Congress of Logic, Methodology and Philosophy of Science, Helsinki.

D. Miller gave spoke at the ETH Zurich Department of Computer Science Distinguished Colloquium Series on 20 April.

S. Graham-Lengrand gave an invited talk at the IFIP Working Group 1.6 on Term Rewriting, on the occasion of its 2015 annual meeting in Warsaw, Poland.

B. Accattoli was an invited speaker at the 16th International Workshop on Logic and Computational Complexity (Kyoto, Japan, 5th of July).

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. He was also the Chair of the LICS 1995 Test-of-Time Award selection committee.

S. Graham-Lengrand is head of the French National Workgroup on *Logic, Algebra, and Computation* (part of GDR Informatique Mathématique, funded by CNRS).

K. Chaudhuri was elected to the Steering Committee of LFMTTP (<http://lfmtp.org>) for a term of 5 years in 2015.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: K. Chaudhuri, “*INF 321 : Les principes des langages de programmation*”, 40 hours eq. TD, L3, École polytechnique, France

Licence: K. Chaudhuri, “*INF 431 : Programmation concurrente et distribuée*”, 40 hours eq. TD, L3, École polytechnique, France

Licence: S. Graham-Lengrand, “*INF411: Les bases de la programmation et de l’algorithmique*”, 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*”, 12 hours, M2, Master Parisien de Recherche en Informatique, France.

Master: D. Miller, “*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*”, 12 hours, M2, Master Parisien de Recherche en Informatique, France.

Licence: T. Libal, “*INF 321 : Les principes des langages de programmation*”, 40 hours eq. TD, L3, École polytechnique, France

Master: T. Libal, “*INF551: Computer-aided reasoning*”, 20 hours eq. TD, M1, École Polytechnique, France.

9.2.2. Supervision

PhD: Zakaria Chihani, “*Certification of first-order proofs in classical and intuitionistic logics*”, École Polytechnique, 2 Nov 2015; supervised by Dale Miller.

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

Internship: Horace Blanc, May-September 2015, supervised by B. Accattoli.

9.2.3. Juries

D. Miller was a reporter and president for the PhD jury of Ali Assaf, École Polytechnique, 28 September.

S. Graham-Lengrand was a member of the PhD thesis committee of Simon Cruanes, École Polytechnique, 10 September.

K. Chaudhuri was a member of the PhD thesis committee of Yuting Wang, University of Minnesota, 5 November.

9.3. Popularization

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

G. Reis participated in “Fête de la Science” as an assistant to the programming activities.

PI.R2 Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organising committees

Yves Guiraud and Philippe Malbos organised with Samuel Mimram (LIX, École Polytechnique) the first edition of the Higher-Dimensional Rewriting and Applications (HDRA) workshop of the International Conference on Rewriting, Deduction, and Programming (RDP), held in Warsaw in June-July 2015. The second edition of HDRA will be held in June 2016 in Porto, during the new Formal Structures for Computation and Deduction (FSCD) conference.

Yann Régis-Gianas, Pierre Letouzey, Matthieu Sozeau were the organisers of the “Ecole de Printemps d’Informatique Théorique 2015” about proof of programs (cf. Highlights section).

Matthieu Sozeau co-organised and chaired the first Coq for Programming Languages (CoqPL) workshop, collocated with POPL’15 in Mumbai, India, in January 2015.

8.1.2. Scientific events selection

8.1.2.1. Member of the conference program committees

Frédéric Loulergue is member of of the program committee of the International Conference on Computational Science (ICCS’15), and is co-chair of the special session “Formal Approaches to Parallel and Distributed Systems” (4PAD) of the Euromicro PDP 2016 conference.

8.1.2.2. Member of the conference steering committees

Pierre-Louis Curien and Hugo Herbelin were members of the steering committee of the conference *Typed Lambda Calculi and Applications* (TLCA) until its merge with the conference *Rewriting Techniques and Application* in the new conference *Formal Structures for Computation and Deduction* (FSCD), whose first edition will be held in Porto in 2016.

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).

Frédéric Loulergue is a member of the steering committee of the international symposium on High-Level Parallel Programming and Applications (HLPP).

8.1.3. Journal

8.1.3.1. Member of the editorial boards

Pierre-Louis Curien is co-editor in chief (and becomes editor in chief in January 2016) of *Mathematical Structures in Computer Science*.

Hugo Herbelin, Pierre Letouzey and Matthieu Sozeau were co-editors of the post-proceedings of the conference TYPES 2014. These post-proceedings were published in October 2015 as LIPICS volume 39.

8.1.3.2. Reviewer - Reviewing activities

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

8.1.4. Invited talks

Pierre-Louis Curien gave an invited talk at the GALOP'15 (Games in Logic and Programming) Workshop, in London (April 11-12).

Matthieu Sozeau participated to the HoTT/UF workshop in Warsaw, Poland (June 29-30). He gave an invited lecture on “Coq support for Homotopy Type Theory”.

Alexis Saurin gave an invited talk, in the form of a distilled tutorial, at WoC'2015, affiliated to ETAPS 2015 on “Logical by need”.

8.1.5. Hiring committees

Pierre-Louis Curien has been member of the “Comité de Sélection” for a professor position in mathematics at the University Paris Diderot.

8.1.6. Scientific expertise

Pierre-Louis Curien is a member of the Scientific Committee of the CIRM (since June 2013).

8.1.7. Presentation of papers

Amina Doumane presented [24] at CSL (sep 2015).

Matthieu Sozeau has presented [31] at ICFP 2015.

Cyprien Mangin has presented [29] at LFMTTP 2015.

Yann Régis-Gianas has presented [32] at Formalize 2015.

Thibaut Girka has presented [33] at ATVA 2015.

Jovana Obradović has presented [43] at Category Theory 2015.

8.1.8. Other presentations

Matthieu Sozeau gave a talk on the development of Coq at the CoqPL workshop in Mumbai (Jan 2015).

Amina Doumane gave a talk at GALOP'15 on Least and Greatest Fixed Points in Ludics.

Étienne Miquey gave a talk at GALOP'15 Workshop on realisability games for arithmetical formulæ [37], and a talk on a classical sequent calculus with dependent types at TYPES'15 [34].

Hugo Herbelin gave a talk at TYPES'15 on a proof of Gödel's completeness using side-effects.

Hugo Herbelin gave a talk at the workshop HoTT-UF15 on an extension of his construction of semi-simplicial types to simplicial types.

Pierre-Louis Curien and Jovana Obradović gave talks at the workshop Logic and Applications 2015 <http://imft.ftn.uns.ac.rs/math/cms/LAP2015>, Dubrovnik (September 21-25).

Cyrille Chenavier and Jovana Obradović gave talks at the workshop HDRA, Warsaw (cf. Scientific events organisation).

8.1.9. Talks in seminars

Yves Guiraud gave talks on various aspects of Squier's theory and its applications in algebra at the LCR seminar (Jan. 2015, LIPN, Univ. Paris 13), the Logique et Interactions seminar (Nov. 2015, I2M, Univ. Aix-Marseille) and the Chocla monthly meeting (Dec. 2015, ENS Lyon).

Étienne Miquey gave talks on the classical realisability and arithmetical formulæ at the Chocla monthly meeting (May 2015, ENS de Lyon) and the Logique et Interactions seminar (Jul. 2015, I2M, Univ. Aix-Marseille).

Matthieu Sozeau gave a talk on a new unification algorithm for Coq at the MIT seminar in Boston (April 2015).

Jean-Jacques Lévy gave a talk about Readable proofs of Depth First Search in graphs using Why3, at VALS seminar, Plateau de Saclay (December), and a talk about The cost of usage in the lambda-calculus, at Deducteam seminar, Inria (April), and Journées Choccola at ENS-Lyon (November).

8.1.10. Attendance to conferences, workshops, schools,...

Matthieu Sozeau attended POPL'15, RDP'15, LFMTP'15 and ICFP'15.

Étienne Miquey attended GALOP'15, the “École Jeunes Chercheurs 2015” of the GDR-IM, TYPES'15 and the EPIT spring school.

Hugo Herbelin attended TYPES'15, RDP'15 and ITP'15.

Pierre-Marie Pédrot attended JFLA'15 and LICS'15.

Hugo Herbelin, Pierre Letouzey, Pierre-Marie Pédrot and Matthieu Sozeau attended the first Coq coding sprint as developers communicating their expertise to the participants. Cyprien Mangin attended as participant.

8.1.11. Groupe de travail Théorie des types et réalisabilité

This is one of the working groups of PPS, jointly organised by Hugo Herbelin and Paul-André Melliès, since September 2009. It is held weekly. Matthieu Sozeau joined the organisation in 2014.

The speakers in 2015 were Danko Ilik (Eliminating control operators from classical realisability), Ali Assaf (Tarski and Coq), Maxime Dénès (Coqnut: a formally verified JIT compiler for Coq), Tomer Libal (Regularity in higher-order unification), Andrew Polonsky (Defining equality by induction on type structure), Sergei Soloviev (Isomorphism of Dependent Products in Type Theory: Specifics and Scientific Context), Noam Zeilberger (Functors are Type Refinement Systems), Gabriel Scherer (Which types have a unique inhabitant?), Andrej Bauer (A sound and complete language for type theory with equality reflection), Nicolas Tabareau (Vers un analogue de l'axiome de Giraud en HoTT), Alexandre Miquel (An axiomatic presentation of forcing, or: forcing for the dummies), Danko Ilik (The exp-log normal form of formulas).

8.1.12. Groupe de travail Catégories supérieures, polygraphes et homotopie

Pierre-Louis Curien and Yves Guiraud, together with Cyrille Chenavier, Maxime Lucas and Jovana Obradović actively participate in this weekly working group of PPS, organised by François Métayer since 2009.

8.2. Teaching - Supervision - Juries

8.2.1. 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).

Alexis Saurin chairs LMF1 M2 since September 2013.

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.

In addition to his regular teaching duties for the Computer Science department of Paris 7 (M1 and M2 Pro), Pierre Letouzey taught 2 courses in the LMF1 M2 in 2015 : initiation to formal proofs on computer (24h) and models of programming (24h).

Matthieu Sozeau teaches in the MPRI course on Advanced uses of Proof Assistants (12 hours + a project), together with Assia Mahboubi (Inria SpecFun).

Licence and Master: Lourdes González had a temporary research and teaching position (A.T.E.R) at University Paris 7 for the academic year 2014–2015. During the second semester (Jan - Aug 2015) she was in charge of TP (Travaux pratiques, 44 hours) on the subjects “Projet Informatique” (L2) and “Introduction aux environnements de développement et génie logiciel” (L3). During the second semester (Jan - Aug 2015) she was in charge of TP (Travaux pratiques, 24 hours) on the subject “Programmation système” (M1).

Licence: Étienne Miquey was in charge of practical sessions in the course “Analyse de données structurées” (36h, L2) and “Programmation Orientée Objet et Interface Graphique” (60h, L2) at University Paris 7.

MOOC: In collaboration with Roberto DiCosmo and Ralf Treinen, Yann Régis-Gianas has created a MOOC about the OCaml programming language.

8.2.2. *Supervision*

Internship: Yann Régis-Gianas has supervised the M2 internships of Béatrice Carré and Jacques Pascal Deplaix, and the M1 internships of Léo Brun and of Loïc Runarvot.

Internship: Matthieu Sozeau has supervised the M2 internships of Gabriel Lewertowsky (with Nicolas Tabareau), who is now starting a PhD under their joint supervision, and of Cyprien Mangin, who is starting a PhD under the supervision of Bruno Barras and Matthieu Sozeau.

Internship: Yves Guiraud has supervised the M2 internship of Pierre Giraud.

PhD in progress: Guillaume Claret, supervised by Hugo Herbelin and Yann Régis-Gianas.

PhD in progress: Thibaut Girka, supervised by Roberto DiCosmo and Yann Régis-Gianas.

PhD in progress: Cyrille Chenavier, supervised by Yves Guiraud and Philippe Malbos.

PhD in progress: Maxime Lucas, supervised by Yves Guiraud and Pierre-Louis Curien.

PhD in progress: Jovana Obradović, supervised by Pierre-Louis Curien.

PhD in progress: Amina Doumane, supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien.

PhD in progress: Étienne Miquey, supervised by Hugo Herbelin and Alexandre Miquel.

Pierre-Marie Pédro and Lourdes González defended their PhD in 2015.

8.2.3. *Juries*

PhD Juries: Pierre-Louis Curien has been reviewer (rapporteur) for the PhD thesis of Fabio Zanasi (Lyon, October 2015).

Examinator tasks: In June and July 2015, Pierre Letouzey has participated to the jury of the competitive examination for the entrance to Ecole Normale Supérieure (ENS Ulm). More precisely, he has been responsible for the oral test of computer science and has been examiner for about forty candidates, one hour each.

8.3. *Popularisation*

Étienne Miquey took part in the animation of several activities about mathematics in primary and high schools of Paris.

Yann Régis-Gianas co-organised the “Journée Francilienne de Programmation”, a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS). Yann Régis-Gianas organised, 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.

Jean-Jacques Lévy gave a presentation about “Science et Informatique” at the primary school le Coteau, Vaucresson (November).

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

Nathalie Bertrand is an elected steering committee member for the international conference QEST (Quantitative Evaluation of Systems).

Thierry Jéron is member of the steering committee of the european summer school MOVEP (Modélisation et Vérification des Systèmes Parallèles). The next edition will take place in Genova in July 2016.

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).

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

Éric Badouel was Scientific President of CRI 2015 (Yaoundé)

Nathalie Bertrand was co-chair of the international workshop QAPL'15 with Mirco Tribastone.

10.1.2.2. Member of the conference program committees

Éric Badouel was PC member of ATAED 2016 (Brussel).

Nathalie Bertrand was PC member of the following international conferences: Formats'15, ICLA'15, QEST'15, TACAS'15.

Loïc Hérouët was member of the program committee of ACSD 2015 (Approaches of Concurrency for Systems Design, Brussels june 2015) and SDL 2015 (System Design Languages, Berlin, 2015).

Thierry Jéron was PC member of the following international conferences: ICTSS'15, TAP'15, USE'15, RV'16.

Hervé Marchand was PC member of the DCDS 2015 and MSR 2015 conferences.

10.1.2.3. Reviewer

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

10.1.3. Journal

10.1.3.1. Member of the editorial boards

Éric Badouel is Editor in Chief of ARIMA Journal.

10.1.3.2. Reviewer - Reviewing activities

Éric Badouel was a reviewer for Science of Computer Programming, Fundamenta Informaticae and Mathematical Review.

Nathalie Bertrand acted as a reviewer for Journal of the ACM, Formal Methods in System Design, Information and Computation.

Éric Fabre reviewed submissions to IEEE TAC, Automatica, J. of Discrete Event Dynamic Systems, IEEE Trans. on Automation Sciences and Engineering.

Loïc Hérouët was a reviewer for Formal aspects of computing and Theoretical Computer Science.

Hervé Marchand was reviewer for JDEDS and for the Annual Reviews in Control.

Christophe Morvan was a reviewer for Journal of Computer and System Sciences and for IEEE Transactions on Automatic Control.

Ocan Sankur was a reviewer for Theoretical Computer Science, Logical Methods in Computer Science, Science of Computer Programming and Formal Methods in System Design

10.1.4. Invited talks

Nathalie Bertrand gave an invited talk at Gandalf 2015, and at MSR 2015. She gave a lecture on Controlling probabilistic systems under partial information at the EJCIM (École jeunes chercheurs Informatique Mathématiques) in april 2015. See the lecture notes [45].

Thierry Jérón and Ocan Sankur both gave lectures at ETR'15 (Ecole temps réel) in Septembre 2015, respectively on "Model-based conformance test generation for timed systems", and "Control of timed systems".

10.1.5. Scientific expertise

Éric Fabre serves as expert for the Minsitry of Research, for the Credit Impot Recherche, a tax-reduction programme for research activities performed by private companies. He was solicited for 4 companies in 2015.

Loïc Hélouët acted as reviewer for the ANR.

Thierry Jérón was reviewer for the CHIST-ERA consortium and for a NSERC Discovery Grant proposal (Canada).

10.1.6. Research administration

Éric Badouel is secretary of the Permanent Committee of CARI, co-Director of LIRIMA, and the Scientific Manager for Africa and Middle-East region at Inria DPEI.

Nathalie Bertrand is secretary and committee member of Gilles Kahn PhD prize.

Éric Fabre is the co-director, with Olivier Audouin, of the joint research lab of Alcatel-Lucent Bell Labs and Inria.

Loïc Hélouët and Éric Fabre are members of the Scientific Board of the joint lab of Alstom Transport and Inria.

Loïc Hélouët was *réfèrent chercheur* for the Inria Rennes research center.

Thierry Jérón was Vice Scientific Delegate of the Inria Rennes research center and member of the Inria Evaluation Committee until 09/2015. This year he was member of the following Inria hiring committees: junior scientists (CR2) at Lille, starting and advanced senior research positions (ARP, SRP), and senior scientists (DR2). He is also member of the IFIP Working Group 10.2 on Embedded Systems and member of the Management Committee (substitute) of the COST IC1402 (ARVI: Runtime Verification beyond Monitoring). He is member of the COS Prospective of Irisa Rennes.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Nathalie Bertrand

Agreg: Responsible of computer science organization, 16h (eq. TD), M2, Ecole Normale Supérieure de Rennes, France.

L3: Lecture on Algorithms, 18h (eq. TD), L3, University Rennes 1, France.

Éric Fabre

Master : "ASR: introduction to distributed systems and algorithms," 12h, M2, Univ. Rennes 1, France.

Master : "Information theory," 15h, M1, Ecole Normale Supérieure de Bretagne, France.

Master : Preparation of Aggregation, 6h, M1, Ecole Normale Supérieure de Bretagne, France.

Blaise Genest

Master: Advanced verification techniques, M2 in Computer Science, Université Rennes I, 10h.

Loïc Hérouët

Licence: JAVA and algorithmics at INSA de Rennes for students in the second year of engineer cycle. He also supervises practical studies (development of a small project by students under the supervision of two teachers).

Agreg: algorithmics at ENS Rennes (8 hours / year).

Éric Fabre, Loïc Hérouët, Hervé Marchand

Master: supervised 3 students from ENS Rennes at the M1 level during 6 month. (2 hours/ week during 6 months)

Christophe Morvan

Licence: Compilation, System, Advanced Algorithmics Université de Paris-Est, Marne-la-Vallée, France.

10.2.2. Supervision

HdR: Nathalie Bertrand, “Contributions to the verification and control of timed and probabilistic models”, University Rennes I, November 16, 2015.

PhD:

Paulin Fournier, “Parameterized verification of networks of many identical processes”, Université Rennes I, December 17, 2015, Supervisors: Nathalie Bertrand, Thierry Jéron, Arnaud Sangnier (LIAFA).

Srinivas Pinisetty, “Runtime Enforcement of Timed Properties”, Université Rennes I, January 23, 2015, Supervisors: Thierry Jéron, Hervé Marchand, Yliès Falcone (LIG).

PhD in progress:

Karim Kecir (2015-2018, CIFRE thesis): “Régulation et robustesse des systèmes ferroviaires urbains”, Université Rennes I, Supervisor: Loïc Hérouët.

Matthieu Pichené (2014-2017): “Stochastic models for the modelling of apoptosis”, Université Rennes I, Supervisor: Blaise Genest.

Engel Lefauchaux (2015-2018): “Information control in probabilistic systems”, Université Rennes I, Supervisors: Nathalie Bertrand, Serge Haddad (LSV, ENS Cachan).

10.2.3. Juries

Éric Badouel was opponent of the Doctoral Thesis of Abel Armas-Cervantès, “Diagnosing Behavioural Differences Between Business Process Models”, University of Tartu, Estonia, August 2015.

Nathalie Bertrand was member of the PhD defense committee of Nathanaël Fijalkow, *Counting and Randomising in Automata Theory*, Université Paris VII, 15/10/2015.

Éric Fabre was in the mid-term jury of 4 PhD students of Telecom Bretagne.

Thierry Jéron was member of the Habilitation defense committee of Nathalie Bertrand, University Rennes I, November 16, 2015 (see above), and president of the PhD defense committee of Abderahman Kriouile, Université de Grenoble, September 17, 2015. He was also in the mid-term PhD jury of Mouna Hkimi (Supélec Rennes).

Hervé Marchand was Member of the PhD Defense of Johan Girault « Conception formelle du pilotage d’une flotte de robots mobiles », Ecole centrale de Nantes, November 2015.

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. Conchon is the program committee co-Chair of ICFEM 2015 (CNAM, Paris, 3-6 November 2015). <http://icfem2015.lri.fr>.
- A. Charguéraud is the organizer of the 2nd International Workshop on Coq for Programming Languages, co-located with POPL, January 23rd 2016. <http://conf.researchr.org/home/CoqPL-2016>.
- A. Paskevich is the co-organizer of the 4th international workshop on Proof eXchange for Theorem Proving (PxTP 2015), affiliated with CADE-25 (August 2-3, 2015, Berlin, Germany).

10.1.1.2. Member of the organizing committees

- S. Boldo and G. Melquiond are members of the organizing committee for the 22nd IEEE Symposium on Computer Arithmetic (ARITH 2015), held in Lyon in June 2015.
- G. Melquiond is a member of the organizing committee for the 23rd IEEE Symposium on Computer Arithmetic (ARITH 23), held in Santa Clara, CA, USA in July 2016.
- S. Conchon is a member of the organizing committee for ICFEM 2015, CNAM, Paris, 3-6 November 2015. <http://icfem2015.lri.fr>.
- S. Conchon is local chair for the 44th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2017), held in Paris, France in January 2017.

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

- A. Charguéraud is program chair for the 2nd International Workshop on Coq for Programming Languages, co-located with POPL, January 23rd 2016. <http://conf.researchr.org/home/CoqPL-2016>.
- A. Paskevich is the co-chair of the 4th international workshop on Proof eXchange for Theorem Proving (PxTP 2015), affiliated with CADE-25 (August 2-3, 2015, Berlin, Germany).

10.1.2.2. Member of the conference program committees

- S. Boldo is a member of the program committee of the 26th Journées Francophones des Langues Applicatifs (JFLA 2015).
- S. Boldo is a member of the program committee of the 8th International Workshop on Numerical Software Verification (NSV-8).
- S. Boldo is a member of the program committee of the 22nd IEEE Symposium on Computer Arithmetic (ARITH 2015).
- S. Boldo is a member of the program committee of the 27th Journées Francophones des Langues Applicatifs (JFLA 2016).
- S. Boldo is a member of the program committee of the 23rd IEEE Symposium on Computer Arithmetic (ARITH 2016).
- A. Charguéraud is a member of the program committee for the 25th European Symposium on Programming (ESOP), to be held in April 2016, <http://www.etaps.org/index.php/2016/esop>.
- A. Paskevich is a member of the program committee of the 20th International Symposium on Formal Methods (FM 2015).

- C. Paulin is a member of the program committee of the 4th ACM-SIGPLAN Conference on Certified Programs and Proofs (CPP 2015, colocated with POPL 2015).
- C. Paulin is a member of the program committee of the conference on Mathematics of Program Construction (MPC 2015).
- C. Paulin is a member of the program committee of the 21st International Conference on Types for Proofs and Programs (Types 2015).
- C. Paulin is a member of the program committee of the 20th International Conferences on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-20).
- C. Paulin is a member of the program committee of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2016).
- C. Paulin is a member of the program committee of the 7th International Conference on Interactive Theorem Proving (ITP 2016).

10.1.2.3. 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 committee of the popular science web site “i()”: <http://interstices.info/>.
- S. Boldo is member of the editorial board of Binaire <http://binaire.blog.lemonde.fr>, the blog of the French Computer Science Society.
- J.-C. Filliâtre is member of the editorial board of the *Journal of Functional Programming*.
- C. Paulin is member of the editorial board of the *Journal of Formalized Reasoning*.

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 was speaker in a panel at the 2015 congress of the French Computer Science Society, on February 4th in Orléans. The panel was about stereotypes and academic orientation of girls.
- S. Boldo gave a talk at the French-Japanese Workshop on Numerical Computations in Paris, on March 25th.
- S. Boldo gave several invited talks in French laboratories: for the Deducteam team (Inria Paris - Rocquencourt) on March 27th, for the Pequan team (UPMC, Paris) on November 30th, at the Digicosme Research Days on March 23rd.
- A. Charguéraud was invited to teach at the Spring School in Theoretical Computer Science, entitled “Mechanizing proofs of programs”, June 26th, <http://www.epit2015.website/>
- C. Marché, “An History of Frama-C”, Frama-C Day, CEA LIST, March 13th, 2015, <http://frama-c.com/framaCDay.html>
- G. Melquiond, “Formal verification of a floating-point elementary function”, ARITH 22 tutorials, June 25th, 2015, <http://www.ens-lyon.fr/LIP/AriC/tutorials-june-25-2015>.
- C. Paulin gave a talk “Langages and systems for interactive proofs” at Collège de France as part of the seminar “Proving programs : why, when and how ?” organised by Gérard Berry <http://www.college-de-france.fr/site/gerard-berry/seminar-2015-03-18-17h30.htm>.
- C. Paulin was invited by FRAE (Fondation de Recherche pour l’Aéronautique et l’Espace, <http://www.fnrae.org/>) to contribute to a panel discussion on how to master complex systems.

- C. Paulin was invited to give a presentation at the Ecole Jeunes Chercheurs Informatique Mathématique (EJCIM 2015, <http://www.univ-orleans.fr/lifo/evenements/EJCIM2015/>) on the Coq proof assistant.

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), 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.
- É. Contejean, leader of the VALS team of LRI since February 2014.

10.1.6. Scientific expertise

- S. Boldo, member of the reviewing board for the ANR (first and second step in 2015, first step in 2016).
- S. Boldo, member of the 2015 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.
- É. Contejean, elected member of the “*section 6 du Comité National de la Recherche Scientifique*” since September 2012.
- C. Marché, member of the “*jury de l’agrégation externe de mathématiques*” as expert in computer science, since 2012.
- C. Marché, president of the evaluation committee of the joint Digiteo-DigiCosme call for projects <https://digicosme.lri.fr/AAPDigiteoDigiCosme2015>. The committee selected 16 thesis projects for funding, among 52 submissions. The committee also selected to support 6 scientific events in the Île-de-France region.
- C. Marché, A. Paskevich, reviewer for the ANR (second step in 2015).

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 70,000 such exercises are solved every month on the website.
- A. Charguéraud is a board member of the non-profit organization *Animath*, which aims at developing interest in mathematics among young students.
- A. Charguéraud and G. Melquiond are members of the committee for the monitoring of PhD students (“*commission de suivi des doctorants*”).
- 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.

- G. Melquiond, elected officer of the IEEE-1788 standardization committee on interval arithmetic since 2008.
- 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_fil/: “Programmation C++11 avancée” (M2), G. Melquiond (18h), “Preuves Interactives et Applications” (M2), C. Paulin (9h), “Vérification déductive de programmes” (M2), A. Paskevich (11.5h), Université Paris-Sud, France.

Licence: “Mathématiques pour l’informatique 2” (L2), C. Paulin (50h), Université Paris-Sud, France.

Licence: “Logique pour l’informatique” (L3), C. Paulin (54h), Université Paris-Sud, France.

Master: “Logique pour l’option informatique à l’agrégation” (M2), C. Paulin (21h), ENS Cachan, France.

Licence: “Programmation fonctionnelle avancée” (L3), S. Conchon (30h), Université Paris-Sud, France.

Licence: “Introduction à la programmation fonctionnelle” (L2), S. Conchon (10h), Université Paris-Sud, France.

Master: “Compilation et langages” (M1), S. Conchon (45h), Université Paris-Sud, France.

Master: “Software Model Checking” (M2), S. Conchon (10h), 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.

DUT (Diplôme Universitaire de Technologie): M1101 “Introduction aux systèmes informatiques” (S1), A. Paskevich (36h), M3101 “Principes des systèmes d’exploitation” (S3), A. Paskevich (58.5h), IUT d’Orsay, Université Paris-Sud, France.

10.2.2. Internships

- S. Conchon supervised the M2 internship of Mattias Roux, who developed a new reachability algorithm for the Cubicle Model Checker.
- A. Charguéraud supervised, with F. Pottier (Inria Paris) the M2 internship of Armaël Guéneau, who developed a formalization in Coq of the big-O notation, and put it to practice to establish big-O asymptotic bounds in CFML, in particular for a sequence data structure with logarithmic-time random access operations.
- C. Paulin supervised with F. Hivert (LRI) the magistère of Mathematics internship of Olivier Stietel, who developed a proof in Coq of a result in combinatorics (a result of Frame, Robinson and Thrall counting the number of Young tableaux of a given shape) using a probabilistic method.

10.2.3. Supervision

PhD: C. Lelay, “Repenser la bibliothèque réelle de Coq : vers une formalisation de l’analyse classique mieux adaptée”, Université Paris-Sud, June 15th 2015, supervised by S. Boldo and G. Melquiond [11].

PhD in progress: S. Dumbrava, “Towards data certification”, since Oct. 2012, supervised by V. Benzaken (LRI) and É. Contejean.

PhD in progress: L. Gondelmans, “Obtention de programmes corrects par raffinement dans un langage de haut niveau”, since Oct. 2013, supervised by J.-C. Filliâtre and A. Paskevich.

PhD in progress: M. Clochard, “A unique language for developing programs and prove them at the same time”, since Oct. 2013, supervised by C. Marché and A. Paskevich.

PhD in progress: 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.

10.2.4. Juries

S. Boldo: reviewer, PhD committee of O. Kupriianova, “Towards a Modern Floating-Point Environment”, Université Pierre et Marie Curie, France, December 2015.

A. Charguéraud: examiner, PhD committee of Lidia Sánchez Gil, “On the equivalence of operational and denotational semantics for parallel functional languages”, Universidad Complutense de Madrid, July 2015.

C. Marché: reviewer, PhD committee of A. Dieumegard, “Formal Guarantees for Safety Critical Code Generation: The Case of Highly Variable Languages”, Université Toulouse 3 Paul Sabatier, France, January 2015.

C. Marché: external reviewer of the PhD memoir of D. Larraz, “Automatic Program Analysis using Max-SMT”, Universitat Politècnica de Catalunya, Barcelona, Spain, April 2015.

C. Marché: president of the PhD committee of A. David, “Vers la synthèse de systèmes ouverts : tableaux pour les logiques temporelles multi-agents”, Université Évry Val d’Essonne, Évry, France, September 2015.

C. Marché: examiner, PhD committee of Z. Chihani, “Certification of First-order proofs in classical and intuitionistic logics”, École Polytechnique, Palaiseau, France, November 2015.

10.3. Popularization

- A. Charguéraud and S. Boldo contributed to the preparation of the exercises of the *Concours Castor informatique* <http://castor-informatique.fr/>. A. Charguéraud is also one of the three organizers of this contest. The purpose of the Concours Castor is to introduce pupils (from *CM1* to *Terminale*) to computer sciences. More than 345,000 teenagers played with the interactive exercises in November 2015.
- C. Marché, together with J. Kanig from AdaCore company, wrote an article in the ERCIM news journal [17] to advertise on the work done in the ProofInUse joint laboratory for the popularization of formal methods in the development of safety-critical Ada programs.

- S. Boldo, with T. Vieville (Mnemosyne team, Inria Bordeaux - Sud-Ouest), F. Masegla (Zenith team, Inria Sophia Antipolis - Méditerranée and P. Bernhard (INRA) wrote a text about the TIPE 2016 (personal work before the competitive entrance in engineering schools). The topic was “Structures: organization, complexity, dynamic”. This was published on the popularization website <http://pixees.fr> [31].
- S. Boldo co-organized popularization talks for the administrative staff of Inria Saclay - Île-de-France. She gave a talk on January 29th about a scientific article [21] and led a coding session (with Scratch) on February 12th with A. Imperiale (M3DISIM team).
- S. Boldo co-organized the coming of teenagers from the collège Flemming in Orsay to the laboratory on May 28th and gave talks to several groups all day long.
- S. Boldo co-organized the Inria Saclay - Île-de-France *Fête de la science*. She created two stands (about programming) and run one on October 9th.
- S. Boldo gave a talk to the winners of the Mathematics Olympiads on June 10th in Rocquencourt.
- S. Boldo gave a talk at the “Girls can code” week on August 27th, in Paris.
- S. Boldo gave a talk to high school teenagers in Angers on October 12th.
- S. Boldo gave a talk to “Classes Préparatoires” at l’Essouriau, Les Ulis on September 24th.
- S. Boldo gave a talk at “Futur en Seine” a popularization festival in Paris and Paris area, in Orsay, on June 18th.
- C. Paulin together with I. Glas from labex DigiCosme is proposing an introduction to computer science (various activities on programming, data representation, algorithms during 6 sessions of 1 hour) as an extracurricular activity in schools for pupils in *CM1-CM2*.
- C. Paulin organised in 2015 the third edition of the Concours ISN of the Labex DigiCosme, supported by the Rectorat de l’Académie de Versailles. Selected projects developed by the high school pupils (Terminale) as part of their curricula in Computer Science are submitted to this contest. The best projects are selected and presented during a general event.
- C. Paulin, I. Glas, and A. Paskevich run a stand (introduction to information technologies and programming) during the “Fête de la science” Île-de-France on October 9 and 10.

VERIDIS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Organization of scientific events

10.1.1.1. General chair, scientific chair

Jasmin Blanchette and Christoph Weidenbach co-organized the [Dagstuhl seminar 15381](#) “Information from Deduction: Models and Proofs” with Nikolaj Bjørner (Microsoft Research, Redmond, USA) and Viorica Sofronie-Stokkermans (Universität Koblenz-Landau, Germany).

Jasmin Blanchette is an ex officio member of the steering committee of the conference series *Interactive Theorem Proving*.

Pascal Fontaine and Thomas Sturm co-organized the [Dagstuhl seminar 15471](#) “Symbolic Computation and Satisfiability Checking” with Erika Abraham (RWTH, Aachen, Germany) and Dongming Wang (Beihang University, Beijing, China).

Stephan Merz is a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS). He chaired the organizing committee of the *Journées Nationales* of the working groups *Géométrie du Calcul, Logique, Algèbre et Calcul*, and *Logique, Types et Preuve* of GDR IM and GDR GPL in October 2015 in Nancy.

Thomas Sturm is chair 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 *Bundeswettbewerb Informatik*, the German competition among high-school students in computer science.

10.1.1.2. Membership in organizing committees

Jasmin Blanchette was co-chair of workshops, tutorials, and system competitions of CADE-25 in Berlin.

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 2015, VTSA took place during the last week of August in Koblenz, Germany.

Dominique Méry and Stephan Merz were part of the organizing committee of the 10th edition of the conference *Modélisation des Systèmes Réactifs* (MSR 2015) in November 2015 in Nancy.

10.1.2. Service in Program Committees

10.1.2.1. Chair of conference program committees

Jasmin Blanchette co-chaired the program committee of the Ninth International Conference on Tests and Proofs in July, as part of the STAF Conference Series in L'Aquila, Italy.

Dominique Méry co-chaired the program committee of the Second Workshop on Formal Integrated Development Environments [38], a satellite of the Formal Methods conference in Oslo, in June 2015.

Stephan Merz co-chaired the program committee of the Second International Workshop on Formal Reasoning in Distributed Algorithms (FRIDA) in June, as part of the DisCoTec federation of conferences in Grenoble, and of the 10th edition of the French conference *Modélisation des Systèmes Réactifs* (MSR 2015) in Nancy.

10.1.2.2. Membership in conference program committees

Jasmin Blanchette served on the program committee of the International Conference on Automated Deduction (CADE).

Pascal Fontaine served on the program committees of the International Conference on Frontiers of Combining Systems (FroCoS) and of the workshop SMT.

Dominique Méry served on the program committees of FM2015, ICTAC 2015, ICECCS 2015, and MEDI 2015.

Stephan Merz served on the program committees of the international conferences ICFEM, NETYS, SEFM, and of the workshops AVoCS, GRSRD, SETS, and SYNASC.

Thomas Sturm served on the program committees of CASC 2015, MACIS 2015, and ISSAC 2015.

Uwe Waldmann served on the program committee of the 11th International Workshop on the Implementation of Logics.

Christoph Weidenbach served on the program committee of the International Conference on Frontiers of Combining Systems (FroCoS).

10.1.3. Editorial boards of journals

Pascal Fontaine, Thomas Sturm, and Uwe Waldmann edited Mathematics in Computer Science 9(3), a special focus volume on *Constraints and Combinations*.

Dominique Méry is a member of the editorial board of the journal *Formal Aspects of Computing* (Springer).

Stephan Merz, together with Jun Pang of the University of Luxembourg, is the editor of a special issue of Formal Engineering Methods in the journal *Formal Aspects of Computing*.

Martin Quinson is a member of the editorial board of the Interstices journal, aiming at increasing the scientific outreach of informatics.

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.

10.1.4. Invited talks

Stephan Merz gave an invited lecture at *Journées Francophones des Langages Applicatifs* in January 2015. He also gave an invited talk at Aarhus University on *Modeling Distributed Algorithms in TLA⁺*.

Thomas Sturm gave an invited talk at FroCoS 2015 titled *From Complete Elimination Procedures to Subtropical Decisions over the Reals*.

Christoph Weidenbach gave an invited tutorial “25th Anniversary of Superposition: Status and Future” at the International Conference on Automated Deduction (CADE), together with Stephan Schulz. He gave an invited tutorial “Automated Reasoning Building Blocks” at the International Conference on Frontiers of Combining Systems (FroCoS).

10.1.5. Leadership within the scientific community

Jasmin Blanchette was elected editor of the newsletter of the Association for Automated Reasoning (AAR) and member of the AAR board.

Pascal Fontaine is one of three SMT-LIB managers. He was elected CADE trustee in October 2014.

Dominique Méry is a member of the IFIP Working Group 1.3 on *Foundations of System Specification*.

Stephan Merz is a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*.

Christoph Weidenbach is a trustee of CADE (elected 2009, reelected 2012).

10.1.6. Scientific expertise

Jasmin Blanchette is an expert for the French Agence Nationale de la Recherche (ANR) and the Deutsche Forschungsgemeinschaft (DFG).

Pascal Fontaine was a panel member for the CASC-25 competition of first-order theorem provers.

Dominique Méry is an expert for the French Agence Nationale de la Recherche (ANR) and for HCERES.

Stephan Merz is an expert for the French Agence Nationale de la Recherche (ANR), for the German DFG, and for the European Research Council (ERC). He helped IRISA Rennes evaluate the opportunity of creating a new research team.

Christoph Weidenbach is an advisor for the German-Israeli Foundation for Scientific Research.

10.1.7. Research administration

Dominique Méry is the head of the Doctoral School IAEM Lorraine for the University of Lorraine and head of the Formal Methods department of the LORIA laboratory.

Stephan Merz is a member of the Scientific Directorate of the International Computer Science Meeting Center in Schloss Dagstuhl. He is the delegate for the organization of conferences at the Inria Nancy – Grand Est research center and head of the PhD committee for computer science of the Doctoral School IAEM Lorraine. He is also the coordinator of the CPER *Sciences du Numérique* in Lorraine (2015–2020).

Thomas Sturm is a member of the selection committee for MSc and PhD students at the International Max Planck Research School.

Christoph Weidenbach is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

10.2. Teaching, Supervision, Juries

10.2.1. Teaching

Licence: Jasmin Blanchette and Daniel Wand, Concrete Semantics with Isabelle/HOL, 60 HETD, Universität des Saarlandes, Germany

Licence: Marie Duflot-Kremer, Algorithmique et Programmation 1, 113 HETD L1 Mathématiques, Informatiques Sciences pour l'Ingénieur, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Projet personnel, 15 HETD, L2 informatique, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Bases de données 2, 10 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.

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 MIAAGE, Université de Lorraine, France.
- Master: Pascal Fontaine, Génie Logiciel, 30 HETD, M1 MIAAGE, IGA Rabbat et Université de Lorraine, Maroc.
- Master: Pascal Fontaine, Procédures de décision et vérification de programmes, 6 HETD, M2 informatique, Université de Lorraine, France.
- Master: Dominique Méry, Models and algorithms, 60 HETD, M1, Telecom Nancy, Université de Lorraine, France.
- Master: Dominique Méry, Modeling and verification of distributed algorithms, 30 HETD, M1, Université de Lorraine, France.
- Master: Dominique Méry, Modeling and verification of distributed algorithms, 30 HETD, M1 informatique, Université de Lorraine, France.
- Master: Dominique Méry, Modeling and verification of software systems, 60 HETD, M1 (continued education), Telecom Nancy, Université de Lorraine, Nancy.
- 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.
- Licence: Martin Quinson, Algorithmique et Programmation, 48 HETD, L3, Telecom Nancy, Université de Lorraine, France.
- Licence: Martin Quinson, Langage C et programmation shell, 48 HETD, L3, Telecom Nancy, Université de Lorraine, France.
- Master: Martin Quinson, Programmation Système, 24 HETD, M1, Telecom Nancy, Université de Lorraine, France.
- Master: Thomas Sturm and Christoph Weidenbach, seminar on decision procedures, Universität des Saarlandes, Germany.
- Master: Uwe Waldmann, Automated Reasoning, 90 HETD, Universität des Saarlandes, Germany

10.2.2. Supervision

- PhD: Manamiary Andriamiarina, Développement d'algorithmes répartis corrects par construction, Université de Lorraine. Supervised by Dominique Méry, defended on October 20, 2015.
- PhD: Marion Guthmuller, Dynamic verification of distributed applications, using a model-checking approach, Université de Lorraine. Supervised by Martin Quinson and Sylvain Contassot-Vivier, defended on June 29, 2015.
- PhD: Manuel Lamotte Schubert, Automatic Authorization Analysis, Saarland University. Supervised by Christoph Weidenbach, defended on September 18, 2015.
- PhD: Martin Suda, Resolution-based Methods for Linear Temporal Reasoning, Universität des Saarlandes. Supervised by Christoph Weidenbach, defended on October 16, 2015.
- PhD in progress: Noran Azmy, On the Automation of Proofs in TLAPS, Saarland University. Supervised by Stephan Merz and Christoph Weidenbach, since 11/2012.
- PhD in progress: Haniel Barbosa, Refutational Completeness in Satisfiability Modulo Theories, Université de Lorraine and UFRN (Natal, Brazil). Supervised by David Déharbe, Pascal Fontaine, and Stephan Merz, since 12/2013.
- PhD in progress: Gabor Alági, Efficient Reasoning in Finite Domains, Saarland University. Supervised by Christoph Weidenbach, since 11/2012.

PhD in progress: Martin Bromberger, Arithmetic Reasoning, Saarland University. Supervised by Christoph Weidenbach, since 07/2014.

PhD (on hold for personal reasons): Pablo Federico Dobal, Satisfiability Modulo Arithmetic Theories, Université de Lorraine and Saarland University. Supervised by Pascal Fontaine, Stephan Merz, and Thomas Sturm, since 09/2014.

PhD in progress: Mathias Fleury, Formalization of Logical Calculi, Saarland University. Supervised by Christoph Weidenbach and Jasmin Blanchette, since 09/2015.

PhD in progress: Marek Košta, Computational Logic, Universität des Saarlandes. Supervised by Thomas Sturm, since 11/2011.

PhD in progress: Marco Voigt, Decidable Hierarchic Combinations, Saarland University. Supervised by Christoph Weidenbach, since 11/2013.

PhD in progress: Daniel Wand, First-Order Extensions to Support Higher-Order Reasoning, Saarland University. Supervised by Christoph Weidenbach, since 02/2011.

10.2.3. Thesis committees

Dominique Méry served as PhD examiner at IRIT.

Stephan Merz served as a reviewer for the PhD theses of Luís Diogo Couto (Aarhus University, Denmark), Hugues Evrard (University of Grenoble), Laure Millet (University Pierre et Marie Curie, Paris), and Alexander Schimpf (University of Freiburg, Germany).

Uwe Waldmann served as a reviewer for the PhD thesis of Simon Cruanes (École Polytechnique).

10.3. Popularization

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

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

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

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

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

CARTE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- Guillaume Bonfante and Jean-Yves Marion participated to the organisation of the partnership meeting between JAIST and LORIA in Nancy, October 2015
- Simon Perdrix has been member of the organizing committee of the Workshop of the Groupe de Travail informatique Quantique in Grenoble 26-27 November 2015.
- Simon Perdrix has been member of the organizing committee of the Workshop of the Groupe de Travail GeoCal-LAC-LTP in Nancy 12-14 October 2015.

9.1.2. Scientific events selection

9.1.2.1. Member of the conference program committees

- Guillaume Bonfante was co-chair of the 8th international symposium on foundation and practice of security 2015.
- Guillaume Bonfante was in the Program Committee of Protection and Reverse Engineering Workshop 2015.
- Guillaume Bonfante was in the Program Committee of the workshop on Logic and Computational Complexity (LCC) 2015.
- Emmanuel Jeandel was in the Program Committee of Computability in Europe (CiE) 2015.
- Jean-Yves Marion was in the Program Committee of the 8th international symposium on foundation and practice of security 2015.
- Jean-Yves Marion was in the Program Committee of Protection and Reverse Engineering Workshop 2015.
- Romain Péchoux was in the Program Committee of FOundational and Practical Aspects of Resource Analysis (FOPARA) 2015.
- Simon Perdrix was in the Program Committee of Asian Quantum Information Science Conference (AQIS) 2015.
- Simon Perdrix is in the Program Committee of Quantum Physics and Logic (QPL), forthcoming: QPL'16 in Glasgow in June 2016.

9.1.2.2. Reviewer

Mathieu Hoyrup reviewed articles for:

- MFCS 2015
- STACS 2015

Emmanuel Jeandel reviewed articles for:

- MFCS 2015
- STACS 2015

Romain Péchoux reviewed articles for:

- FOPARA 2015
- ISMVL 2015
- FOSSACS 2016

Simon Perdrix reviewed articles for:

- AQIS 2015
- ICALP 2015
- LICS 2015
- QPL 2016

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

Emmanuel Hainry reviewed articles for:

- *Theoretical Computer Science*
- *Applicable Analysis and Discrete Mathematics*

Mathieu Hoyrup reviewed articles for:

- *Journal of Symbolic Logic*
- *Information and Computation*
- *Mathematical Structures in Computer Sciences*
- *Logical Methods in Computer Science*
- *Theory of Computing Systems*

Emmanuel Jeandel reviewed articles for:

- *Discrete Mathematics and Theoretical Computer Science*
- *Ergodic Theory and Dynamical Systems*

Romain Péchoux reviewed articles for:

- *Computability - Journal of the association Computability In Europe*
- *Information and Computation*

Simon Perdrix reviewed articles for:

- *Quantum Information and Computation*

9.1.4. Invited talks

- Guillaume Bonfante was invited to give a talk on implicit complexity within NC at the Shonan Meeting on Low Level Code Analysis and Application to Computer Security.
- Mathieu Hoyrup was invited to give a talk at the annual workshop Continuity, Computability, Constructivity (CCC 2015) in Kochel am See, Germany, September 2015.
- Simon Perdrix was invited to give a talk:
 - “The ZX Calculus is incomplete for Clifford+T quantum mechanics”, at "Quantum Theory: from foundations to technologies – QTFT", Vaxjo, Sweden, June 2015,
 - “Supplementary of Interacting Frobenius Algebras” at the Workshop on “Higher topological quantum field theory and categorical quantum mechanics” Erwin Schrödinger International Institute, Vienna, October 2015
 - “Informatique quantique et théorie des graphes” at Journées Graphes et Algorithmes 2015, Orléans, Novembre 2015.

9.1.5. Scientific expertise

Romain Péchoux is external expert for the European commission Horizon 2020 program.

9.1.6. Research administration

Isabelle Gnaedig is:

- vice-leader of the team Carte.

Emmanuel Hainry is:

- member of the CNU (Conseil National des Universités), Section 27.
- organizer of the Carte Seminar.

Mathieu Hoyrup is:

- principal investigator of a PHC Imhotep with Walid Gomaa (Alexandria E-Just University).
- organizer of the Formal Methods Seminar at Loria.

Romain Pécoux is:

- responsible of the Project-team Carte activity report 2015.
- principal investigator of the Inria associate team Acra proposal.

Simon Perdrix is:

- responsible of GT IQ (groupe de travail Informatique quantique) at the CNRS GdR IM (groupe de recherche Informatique Mathématique).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Unless explicitly stated, the teachings below are given at Université de Lorraine.

Licence:

- Guillaume Bonfante
 - Java, L3, Mines Nancy
- Emmanuel Hainry
 - Operating Systems, 30h, L1, IUT Nancy Brabois
 - Algorithmics, 40h, L1, IUT Nancy Brabois
 - Dynamic Web, 60h, L1, IUT Nancy Brabois
 - Databases, 30h, L1, IUT Nancy Brabois
 - Object Oriented Languages, 12h, L2, IUT Nancy Brabois
 - Complexity, 30h, L2, IUT Nancy Brabois
- Mathieu Hoyrup
 - Programmation C, 15h, L1 PACES
 - Programmation JAVA, 56h, L1, IUT Charlemagne
- 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 Pécoux
 - 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.
- Simon Perdrix

- Structure de données, 72h, L1, IUT Charlemagne
- Licence : Modelling Using Graph Theory, 15h, L3 Informatique

Master:

- Guillaume Bonfante
 - Modelling and UML, M1, Mines Nancy
 - Video Games, M1, Mines Nancy
 - Semantics, M1, Mines Nancy
 - Safety of Software, M2, Mines Nancy
- Isabelle Gnaedig
 - Design of Safe Software, Coordination of the module, M2, Telecom-Nancy
 - Rule-based Programming, 20h, M2, Telecom-Nancy
- Emmanuel Hainry
 - Implicit Complexity, 15h, M2 Informatique
- 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

9.2.2. Supervision

PhD in progress: Hubert Godfroy, Semantics of Self-modifying Programs, Jean-Yves Marion (director).

PhD in progress: David Cattanéo, Combinatorial Modelization in Quantum Computation and Generalized Cover Problems, Pablo Arrighi (director), Simon Perdrix (co-advisor).

PhD: Thanh Dinh Ta, 11 May 2015, Malware Algebraic Modeling and Detection, started Sept. 2010, Jean-Yves Marion (director) and Guillaume Bonfante (co-advisor).

PhD: Aurélien Thierry, 11 March 2015, Morphological Analysis of Malware, Jean-Yves Marion (director).

PhD in progress: Paul Bakouche, Mesure de complexité en topologie de petites dimensions, Florian Deloup (co-advisor) and Guillaume Bonfante (director).

9.2.3. Juries

Isabelle Gnaedig was:

- member of the Inria hiring committee for young researchers,
- member of the Telecom-Nancy engineering school admission committee.

Emmanuel Jeandel was:

- Reviewer and Examiner of Simon Martiel's PhD Defense on "Approches informatique et mathématique des dynamiques causales de graphes", defended in Université de Nice Sophia Antipolis, July 6th 2015
- Reviewer of Ilkka Törmä's PhD on "Structural and Computational Existence Results for Multidimensional Subshifts", defended in Turku (Finland), July 31st 2015
- Reviewer of Rodrigo Torres' PhD on "Some Dynamical Properties of Turing Machines Dynamical Models", to be defended in January 2016, Santiago de Chile (Chile)

9.3. Popularization

- Isabelle Gnaedig is member of the scientific vulgarization committee of Inria Nancy - Grand Est. This committee is a choice and guidance instance helping the direction of the center and the person in charge of popularization events to elaborate a strategy, to realize events and to help researchers to get involved in various actions aiming at popularizing our research themes, and more generally computer science and mathematics.
- Mathieu Hoyrup wrote an article on his recent work for Images des Mathématiques.

CASSIS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

The CNIL (Commission Nationale Informatique et Liberté) has official recommendations in terms of electronic voting⁰. These recommendations influence the design of e-voting systems that are deployed in France. However, some of the recommendations seem a bit outdated and dedicated to particular classes of systems. Even more importantly, the CNIL recommendations focus on vote privacy but do not say much about verifiability. Véronique Cortier, David Galindo, and Stéphane Glondu have formulated new recommendations, submitted to the CNIL. They have met some CNIL members to discuss how to integrate some of the propositions to the new version of the CNIL recommendations that should appear in 2016.

10.1.1. Scientific Events Selection

10.1.1.1. Program Committee Chair

- Véronique Cortier: HotSpot 2016
- Frédéric Dadeau: AFADL 2015
- Steve Kremer: GRSRD 2015, GRSRD 2016
- Michaël Rusinowitch: IWSPA 2016

10.1.1.2. Program Committee Member

- Véronique Cortier: Concur 2015, LICS 2015, POST 2015, EuroS&P 2016, SAC 2016, MFCS 2016, E-VoteID 2016, Concur 2016.
- Christophe Ringeissen: CADE-25, FroCoS 2015, WRLA 2016, UNIF 2016, IJCAR 2016.
- Frédéric Dadeau : AMOST 2015, AFADL 2015, QSR 2015
- Abdessamad Imine : DEXA 2015, ICEIS 2015, DASFAA 2015, DEXA 2016, ICEIS 2016
- Steve Kremer : CSF 2016, AsiaCCS 2016, ACISP 2016, AsiaCCS 2015, ESORICS 2015, FCS 2015, TGC 2015.
- Michaël Rusinowitch: TGC 2015, LPAR 2015, CRISIS 2015, PAS 2015, POST 2016.
- Fabrice Bouquet : AMOST 2015, MODEVVA 2015

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.
- Olga Kouchnarenko: Modelling and Analysis of Information Systems (Russian Academy of Science and Springer partnership).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

⁰<http://www.cnil.fr/documentation/deliberations/deliberation/accessible/non/delib/249/>

- Summer School:
 - Véronique Cortier, Summer School École Jeunes Chercheurs en Programmation (EJCP 2015), Nancy, France, June 2015 and Summer School Marktoberdorf 2015, Marktoberdorf, Germany, August 2015.
 - Frédéric Dadeau, Summer School École Jeunes Chercheurs en Programmation (EJCP 2015), Nancy, France, June 2015
- Continuing Education: Fabrice Bouquet, How to Realize Test (audience: CNRS / Inria employees), Marseille, France, 8 october and 1 december 2015
- Master:
 - Fabrice Bouquet, Functional Testing, 18 hours, M2 Computer science, Franche-Comté University, France.
 - Fabrice Bouquet, Artificial Intelligence, 42 hours, M1 Computer science, Franche-Comté University, France.
 - Véronique Cortier, Security of flows, 20 hours, M2 Computer Science, Telecom Nancy and Mines Nancy, France.
 - Frédéric Dadeau, Structural testing, 9 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Alain Giorgetti, Program Proofs, 58 hours, M1 Computer science, Franche-Comté University, France.
 - Alain Giorgetti, Decision Procedures, 13 hours, M2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Specification, Verification and Validation, 12 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Security and Components, 10.5 hours (ETD), M2 Computer science, Franche-Comté University, France.
 - Steve Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Lorraine University, France.
 - Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, Lorraine University, France.
 - Christophe Ringeissen, Decision Procedures for Software Verification, 24 hours (ETD), M2 Computer science, Lorraine University, France.
 - Laurent Vigneron, Security of information systems, 22.5 hours (ETD), M2 Computer science, Lorraine University, France.
 - Laurent Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Lorraine University, France.
- Licence:
 - Alain Giorgetti, Logics and Deduction, 52 hours, L2 Computer science, Franche-Comté University, France.
 - Olga Kouchnarenko, Formal Languages, 60 hours (ETD), L3 Computer science, Franche-Comté University, France.
- E-Learning:
 - Fabrice Bouquet, Artificial Intelligence, 78 hours (ETD), M1 Computer science, Franche-Comté University, France.
 - Fabrice Bouquet, Specification Validation and Test, 39 hours (ETD), M2 Computer science, Franche-Comté University, France.

Alain Giorgetti, Formal Methods, 81 hours, L3 computer science, Franche-Comté University, France.

Olga Kouchnarenko, Languages, Specification and Proof, 25 hours (ETD), L3 Computer science, Franche-Comté University, France.

Olga Kouchnarenko, Compositional approaches in verification, 18 hours (ETD), M2 Computer science, Franche-Comté University, France.

10.2.2. Supervision

- PhD (defended in 2015):
 - Guillaume Scerri, Proof of security protocols revisited, January 29, Hubert Comon-Lundh and Véronique Cortier
 - Bao Thien Hoang, On the Polling Problem for Decentralized Social Networks, February 3, Abdessamad Imine and Christophe Ringeissen
 - Alexandre Vernotte, A pattern-driven and model-based vulnerability testing for Web applications, October 29.
 - Guillaume Petiot, *Contribution à la vérification de programmes C par combinaison de tests et de preuves*, November 4, Jacques Julliand, Nikolai Kosmatov and Alain Giorgetti
 - Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on micro-systems, November 19, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad
- PhD in progress: Younes Abid, Privacy control for social networks, started in March 2015. Abdessamad Imine, Michaël Rusinowitch and Orpailleur co-advising.
 - Hadrien Bride, Validation and Reconfiguration of Modal Petri Nets within Constraint Logic Programming, started in October 2013, Olga Kouchnarenko and Fabien Peureux
 - Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune
 - Alicia Filipiak, Design and validation of security services for mobile platforms: smartphones and tablets, started in March 2015, Véronique Cortier
 - Richard Genestier, Formal specification and verification of programs generating structured data, started in October 2012, Alain Giorgetti and Olga Kouchnarenko
 - Jean-Luc Joly, Randomized approaches for validation and verification procedures, started in December 2011, Pierre-Cyrille Héam
 - Éric Le Morvan, Secure composition of cryptographic protocols, started in October 2013, Véronique Cortier
 - Huu Hiep Nguyen, Secure Collaboration in Mobile Social Networks, started in November 2013, Abdessamad Imine and Michaël Rusinowitch
 - Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, Stéphanie Delaune and Steve Kremer

10.2.3. Juries

- Inria evaluation committee (Steve Kremer, Michaël Rusinowitch)
- Jury Junior Research Position Bordeaux (Véronique Cortier)
- Jury Junior Research Position Inria Paris-Rocquencourt (Véronique Cortier)
- Jury Junior Research Position Inria Saclay-IdF (Michaël Rusinowitch)
- Jury Junior Research Position Inria Rennes-Bretagne Atlantique (Steve Kremer)
- Jury Junior Research Position Inria Grenoble-Rhône Alpes (Steve Kremer)

Jury Chair in Computer Security of CNAM Paris (Michaël Rusinowitch)
Jury Prix Région Lorraine for Thesis, Researcher, Science and Society (Michaël Rusinowitch)
Jury Maitre de conférences U. Lorraine (Véronique Cortier)
Reviewer for Henning Schnoor Habilitation, Kiel U., Germany (Véronique Cortier)
Reviewer for Mathilde Duclos PhD, Grenoble (Véronique Cortier)
Reviewer and Chair of the jury for Elio Goettelmann PhD, U. Lorraine (Laurent Vigneron)
Examiner for Edouard Cuvelier PhD, Louvain-la-Neuve, Belgium (Steve Kremer)
Examiner and Chair of the jury for Ali Kassem PhD, Grenoble (Steve Kremer)
Reviewer for Alessandro Bruni PhD, Lingby, Denmark (Steve Kremer)
Examiner for Mathilde Duclos PhD, Grenoble (Steve Kremer)
Reviewer for Kim Pecina PhD, Saarbruecken, Germany (Steve Kremer)
Reviewer for Amira Amira Henaïen PhD, U. Lorraine (Olga Kouchnarenko)
Examiner and Chair of the jury for Alexandre Vernotte PhD, Besançon (Olga Kouchnarenko)
Reviewer for Anis Bkakria PhD, Telecom Bretagne (Michaël Rusinowitch)
Reviewer for Mohammed Bekkouche PhD, U. Nice-Sophia Antipolis (Fabrice Bouquet)

10.3. Popularization

- Vote électronique : un scrutin à sécuriser. Véronique Cortier. *La Recherche*, 504:70-73, October 2015.
- Blog entries for Blog Binaire (*Le Monde*): Attaque à l'italienne (Véronique Cortier), Les bonnes propriétés d'un système de vote électronique (Véronique Cortier and Steve Kremer), Le vote papier est-il réellement plus sûr que l'électronique ? (Véronique Cortier), Qu'est-ce qu'un bon système de vote ? (Véronique Cortier).
- Pour vivre heureux, vivons anonymes. Abdessamad Imine. *MAIF Magazine*, Novembre 2015.

COMETE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

Note: In this section we include only the activities of the permanent internal members of Comète.

9.1.1. Scientific events organisation

9.1.1.1. 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 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.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committee

Catuscia Palamidessi:

has served as PC chair of **LICS 2015**. 30th Annual ACM/IEEE Symposium on Logic in Computer Science. Kyoto, Japan, 6-10 July 2015.

Frank Valencia:

has served as PC chair (with Camilo Rueda and Martin Leucker as co-chairs) of **ICTAC 2015**: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015. Co-located with **11th International Workshop on Developments in Computational Models DCM 2015**.

as general chair of **ICTAC 2015**: The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia Oct 29-31 2015.

9.1.2.2. Member of the conference program committee

Catuscia Palamidessi is/has been a member of the program committees of the following conferences and workshops:

ICTAC 2016. 13th International Colloquium on Theoretical Aspects of Computing Taipei, Taiwan, 24-31 October 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.

ATVA 2015. The 13th International Symposium on Automated Technology for Verification and Analysis. Shanghai, China, 12-15 October 2015.

WPES 2015. The Workshop on Privacy in the Electronic Society. Denver, Colorado, USA, 12 October 2015.

QUEST 2015. The 12th International Conference on Quantitative Evaluation of SysTems. Madrid, Spain, 1-3 September 2015.

LOPSTR 2015. The 25th International Symposium on Logic-Based Program Synthesis and Transformation. Siena, Italy, 13-15 July 2015.

FORTE 2015. The 35th IFIP International Conference on Formal Techniques for Distributed Objects, Components and Systems. Inria Grenoble, France, 2-4 June 2015.

TPDP 2015. Theory and Practice of Differential Privacy London, UK, 18 April 2015.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

PETS 2016: The 16th Privacy Enhancing Technologies Symposium

WWW 2016: 25th World Wide Web conference

ICISSP 2015: 1st International Conference on Information Systems Security and Privacy

PETS 2015: The 15th Privacy Enhancing Technologies Symposium

FCS 2015: Workshop on Foundations of Computer Security

TPDP 2015: 1st workshop on the Theory and Practice of Differential Privacy

QAPL 2015: 13th Workshop on Quantitative Aspects of Programming Languages

APVP 2015: 6ème 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).

PPDP 2015. The 17th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014). Siena, Italy, July 14-16, 2015.

ICLP DC 2015. 11th ICLP Doctoral Consortium.

9.1.2.3. Reviewer

The members of the team reviewed several papers for international conferences and workshops.

9.1.3. Journal

9.1.3.1. 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 the Springer.

Member of the Editorial Board of the **Electronic Notes of Theoretical Computer Science**, Elsevier Science.

Member of the Editorial Board of **LIPICs: Leibniz International Proceedings in Informatics**, Schloss Dagstuhl –Leibniz Center for Informatics.

Konstantinos Chatzikokolakis is:

Editorial board member of the newly established **Proceedings on Privacy Enhancing Technologies** (PoPETs), a scholarly journal for timely research papers on privacy.

9.1.3.2. Reviewer

The members of the team reviewed several papers for international journals.

9.1.4. Other Editorial Activities

Catuscia Palamidessi is/has been:

Co-editor of the special issue on Quantitative Information Flow on **Mathematical Structures in Computer Science**. 2015.

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.

9.1.5. Other Activities

9.1.5.1. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

ETAPS 2015 (Unifying speaker). The European Joint Conferences on Theory and Practice of Software. London, UK, 11-18 April 2015.

QAPL 2015 (Invited speaker). Thirteenth International Workshop on Quantitative Aspects of Programming Languages and Systems. London, UK, 11-12 April 2015.

ICTAC 2015 (Keynote speaker). The 12th International Colloquium on Theoretical Aspects of Computing. Cali, Colombia, 29-31 October 2015.

9.1.5.2. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the **Alonzo Church Award** Committee. Since 2014. This award is for an outstanding contribution to Logic and Computation within the past 25 years.

Member of the Swedish Research Council Committee for Computer Science, 2015. The main duty of this committee is to evaluate and select the grant applications.

President of the selection committee for the **EATCS Best Paper Award** at the ETAPS conferences. Since 2006.

Member of the **EAPLS PhD Award** committee. Since 2010.

9.1.5.3. Service

Catuscia Palamidessi serves as:

Member of the Comité d'Orientation Scientifique et Technique, Groupe de travail Relation Internationales (COST-GTRI). Since November 2007.

Directrice adjointe du LIX, le Laboratoire d'Informatique de l'Ecole Polytechnique. April 2010 - December 2015.

Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. October 2007 - September 2015.

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 two full professor positions at l'Université de Paris VII (Paris Diderot). Spring 2015.

Member of the comité de selection for a position for Maitre de Conférences à l'Université de Lorraine.

Frank Valencia served as:

President of the Selection Committee for the LIX Postdoctoral Fellowship. May - July 2014.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

PhD : Catuscia Palamidessi has been teaching a course for PhD students, on Protection of sensitive information, at the **BISS 2015**, the Bertinoro International Spring School. Bertinoro, Italy. March 2015. Total 13 hours.

PhD: Konstantinos Chatzikokolakis has been teaching a course for PhD students, on Security and Information Flow, at the **ICTAC 2015** Summer School. Cali, Colombia. Oct 2015. Total 5 hours.

Master : Frank D. Valencia has been teaching the masters course "Computability Theory", 60 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2015.

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. 2015-16. Total: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

9.2.2. Supervision

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 in progress (2013-) **Salim Percy**. Ecole Polytechnique. Grant Digiteo-Digicosme. Co-supervised by Frank D. Valencia and Stefan Haar.

PhD in progress (2012-15) **Marco Stronati**. Ecole Polytechnique. Grant EDX Monge. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-15) **Lili Xu**. Ecole Polytechnique and Chinese academy of Science, Beijing, China. Co-supervised by Catuscia Palamidessi and Huimin Li.

9.2.3. Juries

Catuscia Palamidessi has been reviewer for the thesis of the following PhD students:

Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden. June 2015. The thesis is still in progress, Catuscia Palamidessi was reviewer and member of the committee for the half-way thesis defense, that in Sweden is called Licentiate.

Frank Valencia has been a member of the committee board for the following PhD students:

Thierry Martinez, Title of the thesis: *Execution models for Constraint Programming: kernel language design through semantics equivalence..* Advised by Francois Fages. University Paris-Diderot. Defended in Dec 2015.

Jaime Arias, Title of the thesis: *Formal Semantics and Automatic Verification of Hierarchical Multimedia Scenarios with Inter- active Choice..* Advised by Myriam Desainte-Catherine. University of Bordeaux. Defended in Nov 2015.

9.2.4. Other didactical duties

Catuscia Palamidessi is:

Co-responsible of the Master 2 course on Concurrency since 2003, first at the DEA in Theoretical Computer Science (Paris) and then at the MPRI.

External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.

Member of the 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. Since 2014.

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. 2015-16.

DECENTRALISE Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Invited talks

- 19th Workshop on Elliptic Curve Cryptography, on “Cryptography in GUNet: Protocols for a Future Internet for Libre Societies”

8.1.2. Scientific expertise

- IETF 93, on “Special Use Domain Names of P2P Systems”
- IETF 93, on “Knocking down the HACIENDA with TCP Stealth”
- Invited expert for the high-level conference on “Protecting on-line privacy by enhancing IT security and EU IT autonomy” organized by the Civil Liberties Justice and Home Affairs Committee (LIBE) and the Science and Technology Options Assessment Panel (STOA) of the European Parliament, in association with the Luxemburg Presidency of the European Council

8.2. Teaching - Supervision - Juries

8.2.1. Supervision

PhD : Matthias Wachs, “A Secure Communication Infrastructure for Decentralized Networking Applications”, TU Munich, 2015, Christian Grothoff (advisor)

PhD in progress : Bart Polot, “Practical Routing in Overlays”, 2011-, Christian Grothoff (advisor)

PhD in progress : Florian Dold, “Secure payment systems and applications”, 2015-, Christian Grothoff (encadrant), Jean-Louis Lanet (encadrant)

PhD in progress : Alvaro Garcia-Recuero, “Privacy for the Trolls”, 2014-, Christian Grothoff (encadrant)

8.2.2. Juries

- PhD : Michael Kiperberg, “Preventing Reverse Engineering of Native and Managed Programs”, University of JYVÄSKYLÄ, 2015, Pekka Neittaanmäki (supervisor), Nezer Zaidenberg (supervisor), Christian Grothoff (opponent)

8.3. Popularization

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

DICE Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committees

- Stéphane Frénot, French Tech, représentant de la COMUE de Lyon
- Stéphane Grumbach, ANR, Comité de Pilotage Scientifique du Défi 8 « Sociétés innovantes »
- Stéphane Grumbach, scientific committee Global Forum
- Stéphane Grumbach, scientific committee Collège des Bernardins, Journalisme et bien commun à l'heure des algorithmes,
- Stéphane Grumbach, scientific committee BlendWebMix, annual conference, Lyon

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committees

- Stéphane Grumbach, co-chair Seminar Intermediation and Smartness, Anthropocene Curriculum, The Technosphere Issue, Haus der Kulturen der Welt, Berlin, 15-23 April 2016
- Stéphane Grumbach, co-chair Working group on digital sovereignty with UC Berkeley, Chaire Castex, Les Houches 8-10 december 2015.

9.1.3. Invited talks

- Stéphane Frénot, Plateformes d'intermédiations : Le Web, le temps et ... javascript Inforsid, mai 2015

Stéphane Grumbach has given the following invited talks:

- Political challenges of intermediation platforms, Lunch Lecture at TU Delft - Faculty of Technology, Policy and Management, Delft, 16 December 2015
- Libérer les données dans la ville intelligente : de la défiance à la confiance ? Panel Entretiens Jacques Cartier Smart cities, quelles réponses aux aspirations des citoyens ? Lyon, 2 décembre 2015
- Enjeux stratégiques et économiques des données personnelles, Entretiens Jacques Cartier, La vie privée à travers les cultures. Convergences et divergences dans un monde globalisé, Lyon, 30 novembre 2015
- Géopolitique dans l'espace numérique: la place de la Chine, Séminaire de l'Institut d'Asie Orientale, Lyon, 19 novembre 2015
- Challenges of algorithmic intermediation, ECNU, Shanghai, 21 october 2015
- Panel on New Innovation Strategies in a Challenging Global Environment Global Forum, Digitalization, From Disruption to Sustainability, Oulu, 28-29 september 2015
- Des masses de données aux services de masse globalisés, Assemblée Générale constitutive du GdR MaDICS, Groupement de Recherche Masses de Données, Informations et Connaissances en Sciences, Lyon, 24-25 juin 2015
- Place du numérique, le big data, les réseaux et l'intermédiation : une (r)évolution ? Assises scientifiques, département Environnement et Agronomie INRA, Pont Royal en Provence, 3 juin 2015
- Panel on Public data & Private Interests, Who Owns the Data?, An International Conference on Digital Assets, Data Philanthropy and Public Benefit", BIS 2015, Berkeley, May 14th, 2015
- Les bouleversements politiques et économiques dans la société numérique, Conférence de l'Institut des Sciences du Numérique, Hôtel Potocki, Paris, 9, 10 avril 2015 video
- Maître de la Donnée, Maître du monde, avec Gilles Babinet, Congrès Big Data, CNIT, Paris, 10 mars 2015
- Privacy and Big Data, Byte session, Computers Privacy and Data Protection Conference CPDP2015, Brussels, 22 January 2015

Aurélien Faravelon has given the following talk:

- Education in the age of platforms, ECNU, Shanghai, 21 october 2015

9.1.4. Scientific expertise

Stéphane Grumbach has been involved in public hearing in the political sphere

- Stéphane Grumbach, Big Data : création de valeur, enjeux et stratégies de régulation, Cycle "Mutations technologiques, mutations sociales", France Stratégie, Paris, 12 novembre 2015
- Stéphane Grumbach, La place du traitement massif des données (Big data) dans l'agriculture, audition publique de l'OPECST, Assemblée nationale, Paris, 2 juillet 2015
- Stéphane Grumbach, Des données aux plateformes d'intermédiation : une disruption en profondeur, Journée numérique au Sénat, Paris, 11 février 2015

9.1.5. Research administration

Stéphane Grumbach is director of IXXI, the complex Systems Institute.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Stéphane Frénot, Stéphane Grumbach: Twitter, Facebook et le Web2.0, Module INSA Lyon,

INSA, Stéphane Frénot, Agility: A 32 hours optional course on agile software development presenting both iterative (SCRUM) and stream based approaches (LEAN IT). M1. (since 2011)

INSA, Stéphane Frénot, Innovating Project: Supervising 250 hours student project aim at managing innovating projects. Each student group leads its own subject during one semester. All projects and organizational details are publicly available here: <http://tc-pi.fr> M1 (Since 2006)

INSA, Stéphane Frénot, Learn Other Languages: The aim of the course is to improve one's skills in current state-of-the-art programming and discover different ways to develop using mainly web-oriented programming languages. M1 (Since 2013)

Licence : Robert Riemann, INSA, Algorithmique et programmation 1, 27HETD, L1, INSA Lyon, France

Master : Aurélien Faravelon, Réseaux informatiques et recomposition des frontières sociales, 3HETD, M2, EHESS, France

Master : Aurélien Faravelon, Master Biosciences, 3HETD, M1, ENS Lyon, France

Master : Stéphane Grumbach, Le pouvoir aux algorithmes, introduction du Mooc "Villes intelligentes : défis technologiques et sociétaux", MOOC IPL Citylab, 2016

Master : Stéphane Grumbach, Des masses de données à l'intermédiation algorithmique, les grandes plateformes numériques, une disruption politique, Réseaux complexes: une approche interdisciplinaire, ENS Lyon, mars 2015

9.2.2. Supervision

PhD in progress : Etienne Brodu, DataFlow compilation from JavaScript, Jan 2013, Stéphane Frénot

PhD in progress : Robert Riemann, systemes de vote décentralisés, sept 2014, Stéphane Grumbach

9.3. Popularization

- Stéphane Grumbach, Big Data : quel impact sur la relation aux citoyens ? Journée #ComDemainIDF de la Région Ile de France, Paris, 13 octobre 2015
- Stéphane Grumbach, Comment le numérique change-t-il la société ? Cycle de conférences Homo numericus, Fête de la science, Bourg-en-Bresse, 10 octobre 2015
- Stéphane Grumbach, Les données numériques : une nouvelle matière première ? Pint of Science, Lyon, 20 mai 2015
- Stéphane Grumbach, A qui profitent les Big Data? Soirée-débat Et si on en parlait, "La Révolution Big Data : chance ou menace?" Grand Amphithéâtre, Université de Lyon, 28 avril 2015

PRIVATICS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Cédric Lauradoux : GREHACK 2015.

Daniel Le Metayer : La vie privée à travers les cultures: divergences et convergences dans un monde globalisé, Rencontres Jacques Cartier, Lyon, 31 November 2015.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committee

Cédric Lauradoux : GREHACK 2015.

9.1.2.2. Member of the conference program committee

Mathieu Cunche : Trustcom 2015, ICISSP 2015, HotPlanet 2015.

Cédric Lauradoux : Wisec 2015.

Daniel Le Métayer : IWPE 2015, WETICE 2015.

Claude Castelluccia : WISEC 2015, PETS'15.

Marine Minier : WCC 2015.

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 : Cédric Lauradoux, Advanced Topics in Security, 20h, L3, ENSIMAG, France.

Master : Cédric Lauradoux, Introduction to Cryptology, 30h, M1, University of Grenoble, France.

Master : Cédric Lauradoux, Internet Security, M2, University of Grenoble, France.

Master : Claude Castelluccia, Advanced Topics in Security, 20h, M2, Ensimag/University of Grenoble, France.

Master : Claude Castelluccia, Advanced Topics in Security, 15h, M2, Ensimag/INPG, France.

Master : Marine Minier, Security for wireless networks, 20h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, Wireless Security, 6h, M2, INSA-Lyon, France.

9.2.2. Supervision

PhD defended : Gael Thomas, Algebraic Automata in Symetric Cryptography, Marine Minier.

PhD defended : Lukasz Olejnik, Internet Tracking and Profiling, Claude Castelluccia.

PhD in progress : Jagdish Achara, Mobile devices and operating systems from a privacy point of view, October 2013, Vincent Roca and Claude Castelluccia.

PhD in progress : Thibaud Antignac, New solutions for a better privacy, September 2011, Daniel Le Métayer.

PhD in progress : Jessye Dos Santos, Wireless physical tracking, October 2013, Cédric Lauradoux and Claude Castelluccia.

PhD in progress : Amrit Kumar, Privacy and multiparty computation, November 2013, Cédric Lauradoux.

PhD in progress : Vincent Primault, Privacy and geolocated services, November 2013, Cédric Lauradoux.

PhD in progress : 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): Khaoula Dhifallah, Resiliency properties of protocols for WSNs (02/2015 - 07/2015)

Intern (M2): Saikou Fall, Packet Too Big or Too Small ? The PTB-PTS ICMP-based attack against IPsec gateways and tunneling mechanisms (05/2015 - 09/2015)

Intern (M2): Aude Tessier, Etude comparee technico-juridique des lois dites de renseignement (02/2014- 09/2014)

Intern (M2): Leo Letaro, Détection des altération de pages Web (02/2015-07/2015)

Intern (M1): Mathieu Thiery, NeuroAuth-Authenticating People from their Implicit Memory (03/2015 - 09/2015)

Intern (M1): Lenka Kunikova, An efficient implementation of a generic two-party secure computation protocol in the UC framework (02/2015 - 06/2014)

Intern (M1): Jose Paul Dominguez, Tarantula: individual targeting for passphrase attacks (02/2015 - 06/2014)

Intern (M1): Michael Omer, Security and QR-codes (02/2015 - 06/2014)

Intern (M1): Quentin Ricard, Algorithmic complexity attacks against sorting algorithms (02/2015 - 08/2014)

Intern (M1): Jonathan Tournier, Evaluating Forensics Tools (02/2015 - 06/2014)

9.2.3. Juries

PhD : Lukasz Olejnik, Internet Tracking and Profiling, Université de Grenoble, Grenoble, 30/01/2015, Claude Castelluccia.

HDR : Benoît Parrein, Le code à effacement Mojette: applications dans les réseaux et dans le Cloud, Université de Nantes, Nantes, 22/06/2015, Vincent Roca.

PhD : Regina Melo Marin, Enhancing Privacy Protection in Social Network Systems Through Decentralization and Policy Conflict Management, Université de Rennes, Rennes, 07/09/2015, Daniel Le Métayer.

PhD : Paul Mazenc-Lajoie, Réputation et respect de la vie privée dans les réseaux dynamiques auto-organisés, Université de Rennes, Rennes, 25/09/2015, Daniel Le Métayer.

PhD : Koen Decroix, Model-Based Analysis of Privacy in Electronic Services, Université de Leuven, Leuven, 21/10/2015, Daniel Le Métayer.

PhD : Thibaud Antignac, Méthodes formelles pour le respect de la vie privée par construction, INSA Lyon, Lyon, 25/02/2015, Daniel Le Métayer.

PhD : Joëlle Roué, Analyse de sécurité des chiffrements par bloc, 14/10/2015, Université Pierre et Marie Curie, Paris, Marine Minier.

9.3. Popularization

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

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

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

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

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

Article of V. Roca in Interstice, Quand nos smartphones sont espionnés, https://interstices.info/jcms/p_83464/quand-nos-smartphones-sont-espionnes, 09/2015.

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

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

Seminar of C. Lauradoux at the security seminar LORIA, Google Safe Browsing: Security and Privacy, 18/11/2015.

Seminar of C. Lauradoux at GRACE seminar (Inria Saclay), Membership Tests in Security, 18/11/2015.

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

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

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

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

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

PROSECCO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events selection

10.1.1.1. Member of the conference program committees

- ACM POPL – January 2015, Mumbai, India: Karthikeyan Bhargavan
- ACM CCS – October 2015, Denver, USA: Karthikeyan Bhargavan
- ETAPS POST – April 2015, London, UK: Karthikeyan Bhargavan
- ACM SEC@SAC – April 2015, Salamanca, Spain: Karthikeyan Bhargavan
- HotSpot – April 2015, London, UK: Bruno Blanchet

10.1.1.2. Reviewer

- Members of Prosecco reviewed papers for many major conferences and workshops including ACM CCS, ACM POPL, IEEE S&P, etc.

10.1.2. Journal

10.1.2.1. Member of the editorial boards

Associate Editor

- of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers:
Bruno Blanchet

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 9h equivalent TD, master M2 MPRI, universit  Paris VII, France

License: Karthikeyan Bhargavan, INF431, INF421, INF672, INF321, introductory courses at at Ecole Polytechnique, Palaiseau, France

Doctorat: Catalin Hritcu, lectures at University of Saarbruecken, Germany

Doctorat: Catalin Hritcu, F* tutorials at POPL 2015 and ICFP 2015

10.2.2. Supervision

PhD in progress: Evmorfia-Iro Bartzia

Machine-checked program verification for concrete cryptography, started October 2011, supervised by Karthikeyan Bhargavan and Pierre-Yves Strub

PhD in progress: Antoine Delignat-Lavaud

Verified security for web applications, started September 2012, supervised by Karthikeyan Bhargavan

PhD in progress: Jean Karim Zinzindohoue

Analyzing cryptographic protocols and their implementations, started September 2014, supervised by Karthikeyan Bhargavan

PhD in progress: Nadim Kobeissi

Analyzing cryptographic web applications, started February 2015, supervised by Karthikeyan Bhargavan

PhD in progress: Yannis Juglaret
Micro-policies and Secure Compilation,
started September 2015, supervised by Catalin Hritcu

10.2.3. Juries

Rémy Chrétien – Ph.D. – Jan. 11, 2016 – ENS Cachan
Automated analysis of equivalence properties for cryptographic protocols
Bruno Blanchet (reviewer)

Joeri de Ruiter – Ph.D. – Aug. 27, 2015 – Radboud University Nijmegen
Lesson learned in the analysis of the EMV and TLS security protocols
Karthikeyan Bhargavan (reviewer)

Bart van Delft – Licentiate – Mar. 14, 2015 – Chalmers University
Karthikeyan Bhargavan (discussion leader)

10.3. Popularization

10.3.1. Popular Press and Vulnerability Reports

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

10.3.2. Seminars

- Catalin Hritcu: invited talks at CoqPL Workshop (Jan 2015), HP Labs France (May 2015), Inria Rennes (Jun 2015), PLAS Workshop (Jul 2015), Microsoft Research Redmond (Aug 2015), University of Washington (Aug 2015), ML Workshop (Sep 2015), Alcatel-Lucent Bell Labs (Dec 2015)
- Karthikeyan Bhargavan: invited talks at Real World Crypto (Jan 2015), Inria Nancy (Feb 2015), OSSIR Paris (Jun 2015), DefCon Crypto Village (Aug 2015), Catreil Workshop (Oct 2015)