RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2017

Section Dissemination

Edition: 2018-02-19

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

1. ARIC Project-Team 5
2. AROMATH Project-Team 9
3. CARAMBA Project-Team 13
4. CASCADE Project-Team 17
5. DATASHAPE Project-Team 20
6. GAMBLE Project-Team 23
7. GRACE Project-Team 27
8. LFANT Project-Team 30
9. POLSYS Project-Team 33
10. SECRET Project-Team 37
11. SPECFUN Project-Team 43

ARCHITECTURE, LANGUAGES AND COMPILATION

12. CAIRN Project-Team 46
13. CAMUS Team 49
14. CORSE Project-Team 53
15. PACAP Project-Team 57

EMBEDDED AND REAL-TIME SYSTEMS

16. AOSTE2 Team 60
17. HYCOMES Project-Team 62
18. KAIROS Team 64
19. PARKAS Project-Team 67
20. SPADES Project-Team 69
21. TEA Project-Team 72

PROOFS AND VERIFICATION

22. ANTIQUE Project-Team 74
23. CELTIQUE Project-Team 77
24. CONVECS Project-Team 81
25. DEDUCTEAM Project-Team 87
26. GALLIUM Project-Team 89
27. MARELLE Project-Team 91
28. MEXICO Project-Team 93
29. PARSIFAL Project-Team 96
30. PI.R2 Project-Team 99
31. SUMO Project-Team 104
32. TOCCATA Project-Team 108
33. VERIDIS Project-Team 112

SECURITY AND CONFIDENTIALITY

34. CARTE Team 117
35. CIDRE Project-Team 121
36. COMETE Project-Team 130

37. DATASPHERE Team 134
38. PESTO Project-Team 135
39. PRIVATICS Project-Team 138
40. PROSECCO Project-Team 142
41. TAMIS Team 145

ARIC Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of Organizing Committees

Nicolas Brisebarre was a member of the organization committee of JNCF 2017 (Journées Nationales de Calcul Formel) that took place at CIRM, in Luminy in January 2017. There were more than 70 participants.

Claude-Pierre Jeannerod and Nicolas Louvet organized RAIM 2017 (Rencontres "Arithmétiques de l'Informatique Mathématique") at ENS Lyon in October 2017.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Bruno Salvy is a member of the program Committee of AofA2018 (Analysis of Algorithms) and of FPSAC'2019 (Formal Power Series and Algebraic Combinatorics).

Benoît Libert was a program committee member for Eurocrypt 2017 and TCC (Theory of Cryptography Conference) 2017. He is in the program committees of SCN 2018 (Security and Cryptography for Networks) and ACNS 2018 (Applied Cryptography and Network Security).

Nathalie Revol was a member of the program committee for Arith 24, Correctness 2017, CRE 2017 (Computational Reproducibility at Exascale, Workshop of Supercomputing 2017).

Damien Stehlé is in the program committees of PQCrypto 2017 and 2018, Eurocrypt 2017 and 2018, Asiacrypt 2017 and SCN 2018.

Chitchanok Chuengsatiansup is in the program committee of CRYPTO 2018.

Jean-Michel Muller is a member of the board of the Steering Committee of the ARITH (IEEE Symposium on Computer Arithmetic) series of conferences.

Fabien Laguillaumie is a program committee member for Africacrypt 2017, ACISP 2018 and C2SI-SEA 2018.

10.1.3. Journal

10.1.3.1. Member of Editorial Boards

Bruno Salvy is a member of the editorial boards of the *Journal of Symbolic Computation*, of the *Journal of Algebra* (section Computational Algebra) and of the collection *Texts and Monographs in Symbolic Computation* (Springer).

Jean-Michel Muller is a member of the Editorial board of IEEE Transactions on Computers.

Nathalie Revol was guest editor and Jean-Michel Muller was supervising associate editor of a special issue on Computer Arithmetic of IEEE Transactions on Computers [18].

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

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

10.1.4. Invited Talks

Bruno Salvy was an invited speaker at AofA'2017 (Princeton), where he gave a talk on effective methods in the asymptotic analysis of sequences. He also gave an invited plenary talk at FoCM'2017 (Barcelona), on the use of linear differential equations as a data structure. He will be giving a tutorial at STACS'2018 on random generation of combinatorial structures.

Damien Stehlé gave an invited tutorial talk at the ISSAC 2017 conference (Kaiserslautern, Germany), on lattice reduction algorithms. He was an invited speaker at the Africacrypt 2017 conference (Dakar, Senegal), on the Learning With Errors problem and its applications in cryptography.

Jean-Michel Muller gave an invited talk at the 2017 Asilomar Conference on Signals, Systems, and Computers (Pacific Grove, CA, USA), on the analysis and design of algorithms for complex arithmetic.

10.1.5. Leadership within the Scientific Community

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

Nathalie Revol is the chair of the IEEE 1788 group for the standardization of interval arithmetic: a simplified version of the standard, based only on the binary64 format of IEEE-754, has been approved in December 2017 and will be published as IEEE 1788.1.

10.1.6. Scientific Expertise

Paola Boito was a member of the recruitment committees for two associate professor positions in Limoges (mathematics and computer science).

Jean-Michel Muller was a member of the recruitment committee for an associate professor position in Université Grenoble Alpes (computer science).

Jean-Michel Muller is a member of the Scientific committee of CERFACS, Toulouse. Until October 2017 he was a member of the Steering Committee of “Défi 7” (*information and communication society*) of the french Agence Nationale de la Recherche. He is a member of the Scientific Council of CERFACS, Toulouse. In January 2017, he chaired the Evaluation Committee of LIF Laboratory, Marseille.

Nathalie Revol was a member of the visiting committee for the Computer Science Department and the Mathematics Department of Uppsala University, Sweden.

Fabien Laguillaumie was a member of the recruitement committee for an associate professor position in the Université Claude Bernard Lyon 1.

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

10.1.7. Research Administration

Jean-Michel Muller is co-head of the GDR (Groupement de Recherches) IM of CNRS (around 1400 permanent members, www.gdr-im.fr).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

Master: Vincent Lefèvre, *Arithmétique des ordinateurs* (12h), M2 ISFA (Institut de Science Financière et d’Assurances), Université Claude Bernard Lyon 1.

Master: Fabien Laguillaumie, Cryptography, Error Correcting Codes, 150h, Université Claude Bernard Lyon 1 (on CNRS secondment in 2016-2017).

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

Master: Benoît Libert, Cryptography, 12h, ENS de Lyon.

Master: Damien Stehlé, Hard lattice problems, 24h, ENS de Lyon.

Post-graduate: Claude-Pierre Jeannerod and Nathalie Revol, *Arithmétique flottante et erreurs d’arrondi* (3h), École Jeunes Chercheurs et Jeunes Chercheuses en Informatique Mathématique.

Post-graduate: Damien Stehlé, Foundations of lattice-based cryptography, 10h, NTT (Japan).

Post-graduate: Damien Stehlé, Foundations of lattice-based cryptography, 3h, Seoul National University (South Korea).

Professional teaching: Nathalie Revol, *Introduction à l'arithmétique par intervalles* (3h00), École Précis (Précision, Reproductibilité en Calcul et Informatique Scientifique).

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

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

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

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

10.2.2. Supervision

- PhD: Stephen Melczer, *Effective analytic combinatorics in one and several variables*, defended on June 13, 2017, co-supervised by George Labahn (U. Waterloo, Canada) and Bruno Salvy.
- PhD: Marie Paindavoine, *Méthodes de calculs sur des données chiffrées*, defended on January 27, 2017, co-supervised by Fabien Laguillaumie and Sébastien Canard (Orange).
- PhD: Antoine Plet, *Contribution à l'analyse d'algorithmes en arithmétique virgule flottante* [3], defended on July 7, 2017, co-supervised by Nicolas Louvet and Jean-Michel Muller.
- PhD: Valentina Popescu, *Vers des bibliothèques multi-précision certifiées et performantes* [4], defended on july 6, 2017, co-supervised by Mioara Joldes (LAAS) and Jean-Michel Muller
- PhD in progress: Fabrice Mouhartem, *Privacy-preserving protocols from lattices and bilinear maps*, since September 2015, supervised by Benoît Libert.
- PhD in progress: Chen Qiang, *Applications of Malleability in Cryptography*, since September 2016, co-supervised by Benoît Libert, Adeline Langlois (IRISA) and Pierre-Alain Fouque (IRISA).
- PhD in progress: Radu Titiu, *Pseudorandom functions and functional encryption from lattices and bilinear maps*, since January 2017, supervised by Benoît Libert.
- PhD in progress: Weiqiang Wen, *Hard problems on lattices*, since September 2015, supervised by Damien Stehlé.
- PhD in progress: Alice Pellet–Mary, *Cryptographic obfuscation*, since September 2016, supervised by Damien Stehlé.
- PhD in progress: Miruna Rosca, *Hardness of lattice problems over rings*, since January 2017, supervised by Damien Stehlé.
- PhD in progress: Florent Bréhard, *Outils pour un calcul certifié. Applications aux systèmes dynamiques et à la théorie du contrôle*, since September 2016, co-supervised by Nicolas Brisebarre, Mioara Joldeş (LAAS, Toulouse) and Damien Pous (LIP).
- PhD in progress: Ida Tucker, *Conception de systèmes cryptographiques avancés reposant sur des briques homomorphes*, since Octobre 2017, co-supervised by Guilhem Castagnos (IMB, Bordeaux) and Fabien Laguillaumie.
- PhD in progress: Adel Hamdi, *Chiffrement fonctionnel pour le traitement de données externes en aveugle*, since December 2017, co-supervised by Sébastien Canard (Orange Labs, Caen) and Fabien Laguillaumie.

10.2.3. Juries

Bruno Salvy was a reviewer for the HdR of Thomas Cluzeau (Limoges) and for the PhD thesis of Thomas Sibut-Pinote (École polytechnique). He was also a member of the Habilitation committee of Michael Rao (ENS Lyon). He was a member of the recruitment committee for junior researchers at Inria Grenoble.

Benoît Libert was a reviewer for the PhD theses of Florian Bourse (ENS Paris) and Alonso Gonzalez (University of Chile, Santiago). He was the president of the PhD committee of Geoffroy Couteau (ENS Paris), and a member of the PhD committees of Florian Bourse (ENS Paris) and Alonso Gonzalez (University of Chile, Santiago).

Damien Stehlé was a reviewer for the PhD theses of Pierrick Méaux (ENS Paris) and Philippe Moustrou (University of Bordeaux). He was the president of the PhD committee of Thomas Camus (University of Grenoble).

Jean-Michel Muller was the president of the PhD committee of Anastasia Volkova (Pierre et Marie Curie University, Paris), and a member of the Habilitation committee of Nicolas Brisebarre (ENS Lyon).

Fabien Laguillaumie was a reviewer for the PhD thesis of Francisco Vial-Prado (Université Versailles St-Quentin-en-Yvelines) and Laurent Grémy (Université de Lorraine). He was the president of the PhD committee of Thierry Menfenza (ENS Paris and Université de Yaoundé). He was was also a member of the HDR committee of Céline Chevalier (ENS Paris).

10.3. Popularization

Nathalie Revol is a member of the steering committee of the MMI: Maison des Mathématiques et de l'Informatique, and in particular she was involved in the creation of the *Magimatique 2* exhibition. She presented some magic tricks at Bibliothèque Municipale de la Part-Dieu and at MMI for 3 classes during the Science Fair. She gave talks for a large audience during "Forum Maths Vivantes" and for "La tournée de Pi" (mathematical musical, around 600 attendees) (March 2017). As an incentive for high-school pupils, and especially girls, to choose scientific careers, she gave talks at Lycée Ella Fitzgerald (Saint-Romain-en-Gal) and Mondial des Métiers (in February 2017) and during "Journée Filles et Sciences" in Musée des Confluences and "Journée Filles" by INSA Lyon (above 550 attendees in total, March 2017). She co-organized for two "Coding gouters" organized by MixTeen. She co-organized two days on "Info Sans Ordinateur" gathering researchers interested in unplugged activities. She is a member of the editorial committee of Interstices: https://interstices.info. She taught how to disseminate (computer) science for PhD students in a 20h module of *Insertion Professionnelle*.

Bruno Salvy will give a talk at the Collège de France in December 2017 on methods of analytic combinatorics in random generation.

Damien Stehlé hosted a visit at ENS de Lyon by the regional winners of the Alkindi competition (midde highschool and highschool).

AROMATH Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Member of the Organizing Committees

Bernard Mourrain (chair), Evelyne Hubert, André Galligo, Laurent Busé were members of the organizing committee of the conference MEGA (Effective Methods in Algebraic Geometry), held at the University of Nice – Sophia Antipolis, June 12 – 16, 2017.

Laurent Busé organized the first "Learning Week" of the ARCADES Network : « Opportunity Recognition » at Inria Sophia Antipolis, April 3-7, 2017.

Laurent Busé co-oragnized the workshop "Commutative Algebra, Syzygies and Singularities" at the University of Nice, December 4-6, 2017.

Ioannis Emiris and Christos Konaxis organized the 1st software workshop and the Midterm Review meeting of the ARCADES Network in Athens, November 27 to Decemeber 1, 2017.

Evelyne Hubert co-organized the mini-symposium *Symmetry and Structure in Algebraic Computation* in the conference SIAM Algebraic Geometry, July 31st to August 4th Atlanta (USA) as well as the first joint meeting of the London Mathematical Society and the Institute of Mathematics and its Applications *Symmetry and Comptutation*, October 12th London, UK.

Bernard Mourrain co-organized the mini-symposium *Sparse representations from moments* in the conference SIAM Algebraic Geometry, Atlanta July 31st to August 4th.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Laurent Busé was a PC member of MACIS 2017.

Ioannis Emiris was PC member of ACM ISSAC 2017, and is a member of the Advisory Board of MEGA.

Bernard Mourrain was a member of Executive Committee of the conference MEGA 2017.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

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

Evelyne Hubert is associate editor of the Journal of Symbolic Computation (since 2007) and the journal Foundation of Computational Mathematics (since May). She is a reviewer for Mathematical Reviews (since 2016).

9.1.3.2. Reviewer - Reviewing Activities

Laurent Busé reviewed for the journal *Math. Zeitschrift*, the journal *Computer Aided Geometric Design*, the *Journal of Computational and Applied Mathematics*, the journal *ACM Transactions on Graphics*, the *Journal on Applied Algebra and Geometry*, the *Journal of Software for Algebra and Geometry*, the *Journal of Algebra*, the journal *Annales de l'Institut Fourier*, the journal *Algebra & Number Theory*, and the conferences MEGA, ISSAC and MACIS 2017. He also reviewed an application for CIFRE PhD thesis grants for the ANRT.

Ioannis Emiris reviewed for the journals *ACM Transactions on Graphics*, *Discrete Applied Mathematics*, *Discrete & Computational Geometry*, *Graphical Models*, and the conferences MEGA, and ACM Solid & Physical Modeling 2017. He also reviewed applications for H2020 Projects.

Bernard Mourrain reviewed for the journals *Advances in Computational Mathematics*, *Computer Aided Design*, *Computer Aided Geometric Design*, *Computational Methods and Function Theory*, *Computer Methods in Applied Mechanics and Engineering*, *Discrete Applied Mathematics*, *Foundations of Computational Mathematics*, *Journal of Pure and Applied Algebra*, *Linear Algebra and Applications*, *Mathematical Programming*, and for the conferences MEGA, ISSAC. He is also guest editor of the Special Issue of the *Journal Of Symbolic Computation* after MEGA 2017.

Alessandro Oneto reviewed for the journal *Linear and Multilinear Algebra* and for *Mathematical Reviews* (MathSciNet).

Evelyne Hubert reviewed for the journals *Foundation of Computational Mathematics*, *Journal of Symbolic Computation*, *Journal of Algebra*, as well as for the Springer book series *Texts and Monographs in Symbolic Computation* and the conferences MEGA and CASC.

9.1.4. Invited Talks

Laurent Busé was invited to give a talk at the workshop on *Syzygies*, Trento, September 4-9, 2017.

Ioannis Emiris was invited to give a talk at ETH Zurich, Switzerland, in February 2017; and at EU Joint Research Center, Ispra, Italy, in October 2017.

A. Galligo was invited to give a talk at the workshop *Stillman's Conjecture and other Progress on Free Resolutions: (in honor of the sixtieth birthdays of Dave Bayer and Mike Stillman)*, July 17-21, 2017 at the University of California, Berkeley, USA.

Evelyne Hubert gave plenary lectures at the *International Symposium on Orthogonal Polynomials, Special Functions and Applications* (July 3-7 Canterbury, UK) and at the *Journées Nationales du GdR Informatique-Mathématiques* (March 14-16, Montpellier).

Evelyne Hubert was invited to give talks at the first joint meeting of the London Mathematical Society and the Institute of Mathematics and its Applications, *Symmetry and Computation*, October 12th London, UK; the international conference *Integrable systems, symmetries, and orthogonal polynomials*, September 18-22 Madrid, Spain; the workshop *Resultants, Subresultants and Applications* in the SIAM Conference on Algebraic Geometry, July 31st to August 4th Atlanta, USA; the *Symbolic Analysis* workshop in the conference *Foundations of Computational Mathematics*, July 10-19 Barcelona, Spain; the Mathematics Colloquium at University of Kent in Canterbury, February 28th, UK; *Inaugural meeting of the LMS-EMS Applied Algebra and Geometry Research Network*, February 21st Nottingham, UK.

Bernard Mourrain was invited to give a talk at USTC and HFUT, Hefei, China, April 11-12.

Alessandro Oneto was invited to give talks at the Seminario de Geometría Algebraica y Singularidades, BCAM, Bilbao (Spain) on Hadamard decompositions of tensors, May 16, 2017; at the SIAM Conference in Applied and Algebraic Geometry, GeorgiaTech, Atlanta (USA) on Hadamard decompositions of matrices (and tensors), August 02, 2017; at the Algebra and Geometry Seminar, KTH, Stockholm (Sweden) on Combinatorial tools for new questions on planar polynomial interpolation, October 11, 2017; at the workshop Commutative Algebra, Syzygies and Singularities, Nice (France) on A new question on planar polynomial interpolation and line arrangements, December 4, 2017;

9.1.5. Scientific Expertise

Bernard Mourrain was member of the committee of the HCERES for the evaluation of XLIM, Limoges.

Ioannis Emiris was elected member of the Scientific Council of the Hellenic Foundation of Research and Innovation (http://www.elidek.gr), responsible for Informatics and Mathematics.

9.1.6. Research Administration

Evelyne Hubert is a member of the *Conseil Académique de l'Université Côte d'Azur* (since October) and of the *Commission d'Évaluation* (since 2015), and participated to the hiring jury of junior researchers in Inria NGE and RBA.

Laurent Busé is a board member of the (national) labex AMIES (CRI-SAM representative) and a member of the steering committee of the MSI, *Maison de la Modélisation, de la Simulation et des Interactions* of the University Côte d'Azur. He is also an elected member of the CPRH (Commission Permanente de Ressources Humaines) of the math laboratory of the university of Nice, and is the Inria representative at the "Academic Council" and the "Research Commission" of the University of Nice Sophia Antipolis.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence : Ioannis Emiris, Discrete Math, 52 h, L1, U. Athens, Greece.
- Licence : Ioannis Emiris, Software development for algorithmic problems, 52 h, L3, U. Athens, Greece.
- Master : Ioannis Emiris, Computational Geometry, 52h, M1, U. Athens, Greece.
- Master : Ioannis Emiris, Structural Bioinformatics, 52h, M2, U. Athens, Greece.
- Master : Laurent Busé, Geometric Modeling, 27h ETD, M2, EPU of the University of Nice-Sophia Antipolis.
- Master 2: Bernard Mourrain, Computer Algebra, 15h, MDFI, Univ. Aix-Marseille, Luminy.
- Master 2: Bernard Mourrain, Symbolic-Numeric Computation, 6h, Master ACSYON, Limoges.

9.2.2. Supervision

PhD: Elisa Berrini, “Geometric modeling and deformation for automatic shape optimisation” [1], defended in June 2017. CIFRE collaboration with MyCFD. Supervised by Bernard Mourrain and Yann Roux (My-CFD,K-Epsilon).

PhD in progress: Erick Rodriguez-Bazan, Computational Invariant Theory and Applications, CORDI Inria SAM, started in November 2017, supervised by Evelyne Hubert.

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

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

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

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

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

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

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

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

9.2.3. Juries

Anna Karasoulou (U. Athens) defended successfully her PhD in June 2017. She was supervised by I. Emiris, while B. Mourrain was in the three-person supervising committee of the thesis. Both were members of the seven-person exam committee.

L. Busé was a member of the committee of the PhD of Hao Quang Tran entitled *Images et fibres des applications rationnelles et algèbres d'éclatement*, University Pierre and Marie Curie, Paris, France, November 17th.

CARAMBA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

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

10.1.2. Scientific Events Selection

10.1.2.1. Member of steering committees

- Pierrick Gaudry is a member of the steering committee of the Workshop on Elliptic Curve Cryptography (ECC).
- Emmanuel Thomé is a member of the steering committee of the conference series "Algorithmic Number Theory Symposium" (ANTS).
- Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

10.1.2.2. Member of the Conference Program Committees

- Jérémie Detrey was a member of the Program Committee of ECC 2017.
- Pierrick Gaudry was a member of the Program Committee of EUROCRYPT 2017.
- Aurore Guillevic was a member of the Program Commitee of PKC 2018, Latincrypt 2017 and JC2 2017.
- Marine Minier was a member of the Program Commitee of WCC 2017 and JC2 2017.
- Pierre-Jean Spaenlehauer was a member of the Program Commitee of ISSAC 2017.

10.1.3. Journal

10.1.3.1. Reviewer - Reviewing Activities

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

10.1.4. Invited Talks

- Jérémie Detrey was invited to give a talk at the Rencontres "Arithmétique de l'Informatique Mathématique" (RAIM 2017), Lyon, France.
- Aurore Guillevic was invited to give a talk at the Elliptic Curve Cryptography Conference (ECC17), Nijmegen, Netherlands.
- Emmanuel Thomé was invited to give a talk at the Elliptic Curve Cryptography Conference (ECC17), Nijmegen, Netherlands.
- Marine Minier was invited to give a talk at the Journées Nationales du pré-GDR Sécurité, Paris, France and at the CCA seminar, Paris, 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.
- Emmanuel Thomé
  - is a member of the management committee for the research project "CPER Cyberentreprises" (co-chair).
  - is a member of the *Comité Local Hygiène, Sécurité, et Conditions de Travail* of the Inria Nancy – Grand Est research center.
  - was a member of the hiring committee for the 2015 junior research positions (CR2) at Inria Bordeaux.
- Pierrick Gaudry is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
- Pierre-Jean Spaenlehauer is a member of the *Commission développement technologique* (CDT) of the Inria Nancy – Grand Est research center.
- Paul Zimmermann is member of the Scientific Committee of the EXPLOR *Mésocentre*, of the "groupe de réflexion" *Calcul, Codage, Information* of the GDR-IM, of the advisory board of the OpenDreamKit european project, of the scientific council of the LIRMM laboratory in Montpellier, and chair of the organizing committee of the EJCIM (*École Jeunes Chercheurs Informatique Informatique Mathématique*) which will take place in Nancy in 2018.
- Marine Minier is
  - member of the CoS, poste MCF number 27MCF4376, Université de Rouen, November 2017.
  - member of the CoS, poste MCF number 27MCF575, Université de Grenoble Alpes, May 2017.
  - president of the CoS, poste MCF number 27MCF0955, Université de Lorraine, May 2017.
  - member of the CoS, poste MCF number 27MCF4191, Université de Lyon, May 2017.
  - member of the CoS, poste PR number 27PR0154, Université de Toulouse, May 2017.
  - in charge of the redaction for the LORIA of the Impact Project *Digital Trust*.

10.1.6. Research Administration

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Marine Minier, *Sécurité des systèmes d'information*, 40h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

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

Master: Emmanuel Thomé, *Introduction to Cryptography*, 24 hours (lectures + exercises), M1, Télécom Nancy, Villers-lès-Nancy, France.

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

Master: Pierre-Jean Spaenlehauer, *Initiation aux méthodes analytiques de la théorie des nombres, applications à la cryptographie*, 15h eq. TD, M2 Mathématiques MFA, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

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

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

Master: Jérémie Detrey, *Introduction à la cryptographie*, 8 hours (lectures) + 10 hours (tutorial sessions) + 12 hours (practical sessions), Master Spécialisé, École des Mines de Nancy, France.

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

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

2e année École Polytechnique, Aurore Guillevic, *Les bases de la programmation et de l'algorithmique*, (INF411), 32 hours (lab sessions), Palaiseau, France ("chargée d'enseignement").

10.2.2. Supervision

Internship: Léo Barré, *cube attacks and cube testers*, Université de Bordeaux, March–September (6 months), Pierre-Jean Spaenlehauer and Marine Minier.

Internship: Nicolas David, *Impact des racines réelles sur la sélection polynomiale pour le crible algébrique*, ENS Cachan, June–July (6 weeks), Paul Zimmermann.

Internship: Quentin Deschamps, *Étude de la sécurité du logarithme discret dans* $\mathrm{GF}(p^n)$ *lorsque* n *est composé*, ENS Lyon, July–August (6 weeks), Aurore Guillevic.

Internship: Joël Felderhoff, *infrastructures in complex cubic fields*, ENS-Lyon, June–July (6 weeks), Pierre-Jean Spaenlehauer.

Ph.D. in progress: Sandra Rasoamiaramanana, *Délivrance de contextes sécurisés par des approches hybrides*, since May 2017, Ph.D. CIFRE Orange Gardens, Marine Minier.

Ph.D. in progress: Paul Huynh, *analyse et conception de chiffrements authentifiés à bas coût*, since October 2017, Marine Minier.

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

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

Ph.D. defended [1]: Laurent Grémy, *Sieve algorithms for the discrete logarithm in medium characteristic finite fields*, defended on September 29th, 2017, Pierrick Gaudry & Marion Videau.

10.2.3. Juries

Marine Minier: president of the jury of the PhD: *Synchronisation et systèmes dynamiques : application à la cryptographie* defended by Brandon Dravie, July 2017, Université de Lorraine.

Marine Minier: president of the jury of the PhD: *Réseaux de capteurs et vie privée* defended by Jessye Dos Santos, August 2017, Université de Grenoble Alpes.

Marine Minier: president of the jury of the PhD: *Système de détection d'intrusion adapté au système de communication aéronautique ACARS* defended by Eric Asselin, June 2017, Université de Toulouse.

Marine Minier: president of the jury of the PhD: *Probabilistic models of partial enforcement in distributed systems* defended by Jordi Martori-Adrian, June 2017, Université de Lorraine.

Marine Minier: president of the jury of the PhD: *Méthodes de calculs sur les données chiffrées* defended by Marie Paindavoine, January 2017, Université de Lyon.

Emmanuel Thomé: reviewer of the PhD thesis: *Formules de Thomae pour les courbes algébriques résolubles* defended by Alexandre Le Meur, August 2017, Université de Rennes 1.

Paul Zimmermann: member of the jury of the PhD thesis: *Investigations in Computer-Aider Mathematics: Experimentation, Computation, and Certification* defended by Thomas Sibut-Pinote, December 2017, École polytechnique.

10.3. Popularization

- Pierrick Gaudry organized and participated in a debate fed by excerpts from movies on the topic of cryptography and privacy in March 2017. He also gave a podcast interview about electronic voting for Interstices [15].
- Pierre-Jean Spaenlehauer did a short presentation of asymetric cryptography to middle school students who were award winners of the Alkindi competition.
- Paul Zimmermann co-animated a "Math-en-Jeans" atelier with lycée Vauban in Luxembourg city (Luxembourg).

CASCADE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Events and Activities

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

8.1.1.2. Steering Committees of International Conferences

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

8.1.1.3. Other Steering Committees

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

8.1.1.4. Board of International Organisations

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2018)

8.1.2. Scientific Events Selection

8.1.2.1. Program Committee Member

- CT-RSA '17 – 14-17 February (San Francisco, California, USA): David Pointcheval
- TCC '17 – 12-15 November (Baltimore, Maryland, USA): Hoeteck Wee
- ICALP '17 – 10-14 July (Warsaw, Poland): Hoeteck Wee
- Euro S&P '17 – 26-28 Apr (Paris, France) : Hoeteck Wee
- PKC '17 – 28-31 March (Amsterdam, Netherlands): Hoeteck Wee, Georg Fuchsbauer
- ASIACRYPT '17 – 3-7 December (Hong Kong): Georg Fuchsbauer
- ACNS '17 – 10-12 July (Kanazawa, Japan): Georg Fuchsbauer
- Indocrypt '17 – 10-13 Dec (Chennai, India): Georg Fuchsbauer
- Africacrypt '17 – 24-26 May (Dakar, Senegal): Georg Fuchsbauer

8.1.3. Editorial Boards of Journals

Editorial-in-Chief

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

Associate Editor

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Master: David Pointcheval, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS
- Master: Michel Abdalla, David Pointcheval, Cryptography, M2, MPRI
- Master: Damien Vergnaud, Advanced Algebra and Applications to Cryptography, Ecole Centrale Paris
- Master: David Pointcheval, Cryptography, M2, ESIEA
- Bachelor: Georg Fuchsbauer, Cryptologie, 3e année, ESGI

8.2.2. Defenses

- PhD: Thierry Mefenza Nountu, Pseudo-Random Generators and Pseudo-Random Functions : Cryptanalysis and Complexity Measures, ENS, November 28th, 2017 (Supervisor: Damien Vergnaud)
- PhD: Geoffroy Couteau, Zero-Knowledge Proofs for Secure Computation, ENS, November 30th, 2017 (Supervisor: David Pointcheval & Hoeteck Wee)
- PhD: Pierrick Méaux, Hybrid Fully Homomorphic Framework, ENS, December 8th, 2017 (Supervisor: Vadim Lyubashevsky & David Pointcheval)
- HdR: Céline Chevalier, UC-Secure Protocols using Smooth Projective Hash Functions, ENS, December 11th, 2017 (Supervisor: David Pointcheval)
- PhD: Florian Bourse, Functional Encryption for Inner-Product Evaluations, ENS, December 13th, 2017 (Supervisors: Michel Abdalla & David Pointcheval)

8.2.3. Supervision

- PhD in progress: Raphael Bost, Symmetric Searchable Encryption, from 2014, David Pointcheval (with Pierre-Alain Fouque, at Rennes)
- PhD in progress: Rafael Del Pino, Lattice-Based Cryptography – Complexity and Ideal-Lattices, from 2014, Vadim Lyubashevsky
- PhD in progress: Aurélien Dupin, Multi-Party Computations, from 2015, David Pointcheval (with Christophe Bidan, at Rennes)
- PhD in progress: Pierre-Alain Dupont, Secure Communications, from 2015, David Pointcheval
- PhD in progress: Romain Gay, Functional Encryption, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Dahmun Goudarzi, Secure and Fast Cryptographic Implementation for Embedded Devices, from 2015, Damien Vergnaud
- PhD in progress: Louiza Khati, Disk Encryption Modes, from 2015, Damien Vergnaud
- PhD in progress: Michele Minelli, Increased efficiency and functionality through lattice-based cryptography, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Anca Nitulescu, Verifiable Outsourced Computations, from 2015, David Pointcheval
- PhD in progress: Razvan Rosie, Practical Functional Encryption Schemes For the Cloud, from 2015, Michel Abdalla & Hoeteck Wee

- PhD in progress: Quentin Santos, Advanced Cryptography from a Blockchain, from 2015, David Pointcheval
- PhD in progress: Jérémy Chotard, Attribute-Based Encryption, from 2016, David Pointcheval (with Duong Hieu Phan, at Limoges)
- PhD in progress: Michele Orrù, Functional Encryption, from 2016, Hoeteck Wee & Georg Fuchsbauer
- PhD in progress: Balthazar Bauer, Transferable e-Cash, from 2017, Georg Fuchsbauer
- PhD in progress: Chloé Hébant, Big Data and Privacy, from 2017, David Pointcheval (with Duong Hieu Phan, at Limoges)
- PhD in progress: Mélissa Rossi, Post-Quantum Cryptography, from 2017, Michel Abdalla (with Henri Gilbert at ANSSI and Thomas Prest at Thales)

8.2.4. Committees

- PhD Afonso Delerue Arriaga. *Private Functional Encryption* – Luxembourg University - Luxembourg – January 17th, 2017: Michel Abdalla (Examiner)
- HdR Maria Naya-Plasencia. *Symmetric Cryptography for Long- Term Security* – Université Paris VI – France – May 5th, 2017: David Pointcheval (Reviewer)
- PhD Benjamin Richard. *Study of 3-Party Authentication and Key-Derivation Protocols* – Université Rennes 1 - France – August 30th, 2017: Michel Abdalla (Reviewer)
- PhD Thierry Mefenza Nountu. *Pseudo-Random Generators and Pseudo-Random Functions: Cryptanalysis and Complexity Measures* – ENS - France – November 28th, 2017: Damien Vergnaud (Supervisor)
- PhD Geoffroy Couteau. *Zero-Knowledge Proofs for Secure Computation* – ENS - France – November 30th, 2017: David Pointcheval & Hoeteck Wee (Supervisors)
- PhD Britta Hale. *Low-Latency Key Exchange and Secure Channels* – NTNU - Norway – December 5th, 2017: Michel Abdalla (Reviewer)
- PhD Pierrick Méaux. *Hybrid Fully Homomorphic Framework* – ENS - France – December 8th, 2017: David Pointcheval (Supervisor)
- HdR Céline Chevalier. *UC-Secure Protocols using Smooth Projective Hash Functions* – ENS - France – December 11th, 2017: David Pointcheval
- PhD Florian Bourse. *Functional Encryption for Inner-Product Evaluations* – ENS - France – December 13th, 2017: Michel Abdalla & David Pointcheval (Supervisors)

DATASHAPE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- Frédéric Chazal co-organized, with M. Meila 5Univ. of Washington) the NIPS 2017 workshop "Synergies in Geometric Data Analysis", December 2017.
- Frédéric Chazal co-organized the workshop "Functoriality in Geometric Data", Schloss Dagstuhl, Germany, January 2017

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

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

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

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

10.1.3. Invited Talks

Jean-Daniel Boissonnat has been invited and gave a talk at NYU-AD on November 19, 2017.

Frédéric Chazal, Foundations of Computational Mathematics (FoCM'17), Computational Topology and Geometry workshop, Barcelona, Spain, July 2017.

Frédéric Chazal, Applied Topology in Bedlewo 2017 Conference, Bedlewo, Poland, June 2017.

Frédéric Chazal, UC Davis Statistical Sciences Symposium, Davis, USA, May 2017.

Frédéric Chazal, Applied and Computational Algebraic Topology, Hausdorff Institute, Bonn,Germany, April 2017.

Frédéric Chazal, The First International Conference on the Mathematics of Data Science, Hong Kong Baptist University, Hong Kong, March 2017.

Frédéric Chazal, CNA/Ki-Net Workshop: Dynamics and Geometry from High Dimensional Data, Carnegie Mellon University, March 2017.

Frédéric Chazal, Colloquium, collaborative research center Discretization in Geometry and Dynamics, Munich, February 7, 2017.

Frédéric Chazal, Statistics/Learning at Paris-Saclay, workshop at IHES, January 19, 2017.

Mathijs Wintraecken gave an invited talk at the SoCG workshop on Algorithms for the Medial Axis in Brisbane, June 2017.

Steve Oudot, BIRS workshop on Topological Data Analysis: developping abstract foundations, Banff, Canada, August 2017.

Steve Oudot, Mini-Symposium on Computational Topology, Brisbane, Australia, July 2017.

Steve Oudot, Dagstuhl seminar on Topology, computation and data analysis, Dagstuhl, Germany, July 2017.

Steve Oudot, Applied Topology Seminar, Brown University, USA, April 2017.

Steve Oudot, TRIPODS wokshop on Geometry and topology for data, ICERM, USA, December 2017.

Steve Oudot, workshop on Mathematical signal processing and data analysis, Bremen University, Germany, September 2017.

Steve Oudot, Conférence de rentrée Maths-Info, ENS Cachan, September 2017.

10.1.4. Leadership within the Scientific Community

Steve Oudot is co-organizing the monthly seminar on combinatorial and computational geometry at Institut Henri Poincaré.

Steve Oudot is co-head of the GT Géométrie Algorithmique since September 2017.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Collège de France : Jean-Daniel Boissonnat, Géométrie algorithmique: données, modèles, programmes, avril-juin 2017.

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

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

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

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

Master: Frédéric Chazal, Topological Data Analysis, 16h eq-TD, M2, Mathématiques, Vision, Apprentissage (MVA), ENS Paris-Saclay, France.

Winter School on Computational geometry and topology for data analysis, Jean-Daniel Boissonnat, Frédéric Chazal, Sophia-Antipolis, january 2017.

10.2.2. Supervision

PhD: Eddie Aamari, A Statistical Approach of Topological Data Analysis, September 1st, 2017, Frédéric Chazal (co-advised by Pascal Massart).

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

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

PhD: Mathieu Carrière, Topological signatures for geometric data, defended November 21st, 2017, Steve Oudot.

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

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

PhD in progress: Théo Lacombe, Statistics for persistence diagrams using optimal transport, started October 1st, 2017, Steve Oudot.

PhD in progress: Alba Chiara de Vitis, Concentration of measure and clustering, Jean-Daniel Boissonnat and David Cohen-Steiner.

PhD in progress: Siargey Kachanovich, Manifold reconstruction in higher dimensions, Jean-Daniel Boissonnat.

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

PhD in progress: Siddharth Pritam, Approximation algorithms in Computational Topology, Jean-Daniel Boissonnat.

PhD in progress: Raphaël Tinarrage, Persistence and stability of nerves in measured metric spaces for Topological Data Analysis, started September 1st, 2017, Frédéric Chazal and Marc Glisse.

PhD in progress: Vincent Divol, statistical aspects of TDA, started September 1st, 2017, Frédéric Chazal (co-advised by Pascal Massart).

10.2.3. Juries

Frédéric Chazal was a member of the PhD defense committee of Aruni Choudhary, MPI (reviewer) and Aurelien Vasseur (co-advisor).

Jean-Daniel Boissonnat was a member of the PhD defense committee of Eddie Amari.

Steve Oudot was a member (examiner) of the PhD defence committees of Jérémy Dubut and Nicolas Ninin (Cosynus team, Ecole polytechnique).

10.3. Popularization

10.3.1. Inria-Industry Meeting

Marc Glisse, Miro Kramar and Steve Oudot held a booth for half a day.

Marc Glisse played for a small video which is now on the InriaInnovation YouTube channel https://youtu.be/lKNjGk-Z6b4.

GAMBLE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Sylvain Lazard organized with S. Whitesides (Victoria University) the 16th Workshop on Computational Geometry at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

Monique Teillaud co-organized with Claire Mathieu Celebrating Claude Puech's birthday, Paris, June 12.

Monique Teillaud co-organized the workshop Geometric Aspects of Materials Science with Vanessa Robins and Ileana Streinu, Brisbane, Australia, July 4–5.

Monique Teillaud co-organized with the Astonishing partners the Astonishing workshop at Loria/Inria nancy, September 25–26.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Sylvain Lazard was a member of the program committee of SoCG, *Symposium on Computational Geometry*.

Monique Teillaud was a member of the program committee of WADS, *Algorithms and Data Structures Symposium*.

10.1.2.2. 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.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Monique Teillaud is a managing editor of JoCG, *Journal of Computational Geometry* and a member of the editorial board of IJCGA, *International Journal of Computational Geometry and Applications*.

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

10.1.3.2. 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.

10.1.4. Invited Talks

Monique Teillaud was an invited speaker of CATS, *Computational & Algorithmic Topology*, Sydney, Australia, June 27 – July 1st.

Guillaume Moroz was invited to give a talk at the Effective Geometry and Algebra seminar at IRMAR.

10.1.5. Leadership within the Scientific Community

10.1.5.1. Steering Committees

Monique Teillaud is chairing the Steering Committee of the Symposium on Computational Geometry (SoCG). She was a member of the Steering Committee of the European Symposium on Algorithms (ESA) until September.

10.1.5.2. Learned societies

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

10.1.6. Scientific Expertise

Monique Teillaud acted as a reviewer for the DFG, *Deutsche Forschungsgemeinschaft* (German Research Foundation).

10.1.7. Research Administration

10.1.7.1. Hiring committees

Olivier Devillers was the representative of LORIA in the hiring committee for an Associate Professor (MCF) position (IUT St Dié/LORIA) and composed the committee with the president.

10.1.7.2. National committees

L. Dupont is the secretary of *Commission Pédagogique Nationale Carrières Sociales / Information-Communication / Métiers du Multimédia et de l'Internet* (since May).

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

10.1.7.3. Local Committees and Responsabilities

O. Devillers: Elected member to *Pole AM2I* the council that gathers labs in mathematics, computer science, and control theory at *Université de Lorraine*.

L. Dupont Instigator (June 2016) and head of the Bachelor diploma *Licence Professionnele Animation des Communautés et Réseaux Socionumériques*, Université de Lorraine.

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

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

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

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

10.1.7.4. Websites

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Olivier Devillers, *Synthèse, image et géométrie*, 12h (academic year 2017-18), IPAC-R, Université de Lorraine. https://members.loria.fr/Olivier.Devillers/master/

Master: Olivier Devillers and Monique Teillaud, *Computational Geometry*, 24h (academic year 2017-18), Master2 Informatique, ENS Lyon https://members.loria.fr/Monique.Teillaud/Master2-ENS-Lyon/.

Licence: Sény Diatta, *Algorithme et Programmation*, 54h, L1, Université de Lorraine, France.

Licence: Sény Diatta, *Outils Informatiques et Internet*, 42h, L1, Université de Lorraine, France.

Licence: Charles Duménil, *Mathématiques*, 42h, L2, Université de Lorraine, France.

Licence: Charles Duménil, *Logiciel*, 20h, L2, Université de Lorraine, France.

Licence: Charles Duménil, *Algorithmique et programmation avancée*, 34h, M2, Université de Lorraine, France.

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

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

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

Licence: Laurent Dupont *Databases* 30h L3, Université de Lorraine, France,

Licence: Laurent Dupont *Web devloppment and Social networks* 80h L3, Université de Lorraine, France.

Licence: Iordan Iordanov, *Algorithmique et Programmation*, 64h, L1, Université de Lorraine, France.

Licence: Iordan Iordanov, *Systèmes de gestion de bases de données*, 20h, L2, Université de Lorraine, France.

Licence: Iordan Iordanov, *Algorithmique et développement web*, 28h, L2, Université de Lorraine, France.

Licence: Iordan Iordanov, *Programmation objet et événementielle*, 16h, L3, Université de Lorraine, France.

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

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

10.2.2. Supervision

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

PhD in progress: Charles Duménil, Probabilistic analysis of geometric structures, started in Oct. 2016, supervised by Olivier Devillers.

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

PhD in progress: George Krait, Topology of singular curves and surfaces, applications to visualization and robotics, started in Nov. 2017, supervised by Sylvain Lazard, Guillaume Moroz and Marc Pouget.

Postdoc: Vincent Despré, Triangulating surfaces with complex projective structures, started in Nov. 2017, supervised by Monique Teillaud.

10.2.3. Internships

Jian Qian, from Ècole Normale Supérieure Paris, did a L3 internship from Jul 2017 until Aug 2017 co-advised by Guillaume Moroz and Marc Pouget on a topic of ANR SingCAST.

Guillermo Alfonso Reyes Guzman, from Université de Lorraine, did a Master internship from March 2017 until July 2017 advised by O. Devillers on deletion in 3D Delaunay triangulation.

Camille Truong-Allie (Master 1, “research path”, École des Mines de Nancy), Lloyd algorithm in the flat torus, started in October, supervised by Monique Teillaud.

10.3. Popularization

L. Dupont participated to several days of popularization of computerscience: Open Bidouille Camp March, 26th 2017, popularization of programming, general audience ; ISN day March, 30th 2017, popularization of computerscience for high-school teachers ; Fête de la Science 14th October 2017 Inria event, general audience, and Google Day in Nancy 21st October 2017, general audience.

GRACE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

B. Smith was a member of the organizing committee and Short Talk Chair for IEEE EuroS&P 2017 (Paris, April 2017)

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- D. Augot was co-chair of Workshop on Coding and Cryptography (WCC) 2017 at St Petersburg (Russia).

9.1.2.2. Member of the Conference Program Committees

B. Smith: Latincrypt 2017, ECC (International Workshop on Elliptic Curve Cryptography) 2017.

D. Augot and A. Couvreur : Fifth Code-based Cryptography Workshop 2017, Tenerife, Spain.

A. Couvreur: WCC 2017 (Workshop on Coding and Cryptography 2017, St Petersbug, Russia).

A. Couvreur : AGC^{2}T 2017 (Arithmetic Geometry Cryptography and Coding Theory 2017, Marseille, France).

D. Augot: International Conference on Mathematical Aspects of Computer and Information Sciences https://macis2017.sba-research.org/

9.1.2.3. Reviewer

B. Smith: IFIPSEC2017, Africacrypt 2017, WCC 2017, Asiacrypt 2017, Eurocrypt 2017, MACIS 2017, PKC 2018

J. Lavauzelle: MACIS 2017

A. Couvreur: Crypto 2017, Eurocrypt 2017, ISIT 2017.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.

9.1.3.2. Reviewer - Reviewing Activities

B. Smith: Theory of Computing Systems, Springer Women in Mathematics, Research in Number Theory, IEEE Transactions on Information Theory, Journal of Cryptographic Engineering.

A. Couvreur: IEEE Transactions on Information Theory, IEEE Transactions on Communication, Journal of Number Theory, SIAM Journal on Applied Algebra and Geometry.

9.1.4. Invited Talks

B. Smith was an invited speaker at the annual FMF Symposium, a public science event at Universiteit Groningen (Groningen, NL, November 2017)

B. Smith was an invited speaker in the SIAM Applied Algebraic Geometry minisymposium on Applications of Computational Algebraic Geometry to Cryptology (Atlanta, USA, August 2017).

B. Smith was an invited speaker at the FoCM workshop on Computational Number Theory (Barcelona, ES, July 2017)

B. Smith was an invited speaker at the Summer School on Real-World Crypto and Privacy (Sibenik, HR, June 2017)

B. Smith was an invited speaker at JeudiX, a public science outreach event of École polytechnique (Paris, January 2017)

9.1.5. Animation of Seminars

- D. Augot is member of the scientific committee of the CCA seminar, “Codage, Cryptographie et Algorithms”, https://cca.inria.fr
- D. Augot, with Bernadette Charron-Bost, is heading the scientific committee of the Blocksem seminar at Polytechnique, on blockchains, http://www.lix.polytechnique.fr/blocksem
- D. Augot, with Fabrice Le Fessant, organised the Open Source Spring on blockchains http://www.open-source-innovation-spring.org/

9.1.6. Research Administration

F. Morain is vice-head of the Département d’informatique of Ecole Polytechnique.

F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).

A. Couvreur is member of LIX’s *Conseil de laboratoire*.

B. Smith was the International Correspondant for CRI Saclay.

B. Smith was a member of the COST-GTRI.

D. Augot is elected member of the “conseil académique consultatif” de Paris-Saclay.

D. Augot was in the “comité de sélection” for a “maître de conférences” position in Grenoble

D. Augot was heading the “comité de sélection” for a “maître de conférences” position in Rouen

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

B. Smith, Computer Programming (CSE101), 23h EqTD, L1, École polytechnique, France

J. Lavauzelle, 1I001, *Éléments de programmation*, tutorial class (17.5h equiv TD), L1, Université Pierre et Marie Curie

J. Lavauzelle, 2I003, *Initiation à l’algorithmique*, tutorial class (47.5h equiv TD), L2, Université Pierre et Marie Curie

A. Couvreur and E. Barelli, INF411, ”Les bases de la programmation et de l’algorithmique“, 21.3h (equiv TD), 2nd year (L3), Ecole Polytechnique, France.

E. Barelli, INF311, ”Introduction à l’informatique“, 26.7h(equiv TD), 1st year, Ecole Polytechnique, France.

Master:

B. Smith, Advanced Cryptology (INF568), 55h EqTD, M1, École polytechnique, France

B. Smith and F. Morain, Algorithmes Arithmétiques pour la Cryptologie (2-12-2), 20h EqTD, M2, Master Parisien de Recherche en Informatique (MPRI), France

A. Couvreur and F. Morain, Introduction to Cryptology (INF558), 40h, M1, École polytechnique, France

A. Couvreur, Error Correcting Codes and Applications to Cryptography, (2-13-2), 15h, M2, MPRI, FRANCE

Master 2 intern

- D. Augot was the director of Rémi Clarisse internship on the Chor-Rivest cryptosystem

Students project

- D. Augot was managing two groups of polytechniques students on their own project: one about a voting system based on homomorphic encryption (with CEA List), the second about a medical kidney exchange scheme secured and enforced by the Hyperledger/fabric blockchain (with Orange)

9.2.2. Supervision

PhD : Cyril Hugounenq, Volcans et calcul d'isogénies, Université Paris Saclay, 25/09/2017, F. Morain& L. Goubin & L. De Feo.

9.2.3. Juries

- D. Augot
  - examinator of the PhD defense of Sarah Kamel, "Sécurité pour les réseaux sans fil", le 10 mars 2017 (Télécom Paris Tech)
  - examinator of the PhD defense of Francisco Vial-Prado, "Contributions to the design and analysis of fully homomorphic encryption schemes, le 12 juin 2017 (Université Versailles Saint-Quentin)
  - examinator of the PhD defense of Vlad Dragoi "Approche algébrique pour l'étude et la résolution de problèmes algorithmiques issus de la cryptographie et de la théorie des codes", le 6 juillet 2017 (University of Rouen).
  - examinator of the PhD defense of Mohamed A. M. Saeed Taha "Algebraic Approach for Code Equivalence", le 18 décembre 2017 (University of Rouen).
- A. Couvreur
  - PhD : Hervé Talé Kalachi (University of Rouen).
  - Agrégation de Mathématiques.

9.3. Popularization

- A. Couvreur gave the *Conférence inaugurale* of the *Semaine des mathématiques* in the accadémie de Créteil: *Cryptographie, le langage des secrets*.

LFANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

B. Allombert and K. Belabas organized a workshop PARI/GPin Lyon on 09-13 January 2017.

B. Allombert and K. Belabas organized a workshop “Elliptic curves, modular forms and L-functions in the PARI/GPsystem” in Clermont-Ferrand on 19-23 June 2017.

B. Allombert and A. Page organized a mini-workshop PARI/GPin Oujda, Morocco on 22-23 November 2017.

8.1.2. Journal

8.1.2.1. Member of the Editorial Boards

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

H. Cohen is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM)*.

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

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

8.1.3. 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.

K. Belabas is a member of the ’conseil scientifique’ of the Société Mathématique de France

8.1.4. Research Administration

Since January 2017, A. Enge is “délégué scientifique” of the Inria research centre Bordeaux–Sud-Ouest. As such, he is also a designated member of the “commission d’évaluation” of Inria.

Since January 2015, K. Belabas is vice-head of the Math Institute (IMB). He also leads the computer science support service (“cellule informatique”) of IMB and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

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

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

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

Since January 2015, J.-M. Couveignes is the head of the Math Institute (IMB). He is head of the Scientific Committee of the Albatros (ALliance Bordeaux universities And Thales Research in AviOnicS) long term cooperation between Inria, Bordeaux-INP, Université de Bordeaux and CNRS.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

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

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

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

Master : K. Belabas, *Computer Algebra*, 91h, M2, University of Bordeaux, France;

Licence : Jean-Paul Cerri, Arithmétique et Cryptologie, 24h TD, L3, Université de Bordeaux, France

Licence : Jean-Paul Cerri, Algèbre bilinéaire et géométrie, 35h TD, L3, Université de Bordeaux, France

Licence : Jean-Paul Cerri, Structures algébriques 2, 35h TD, L3, Université de Bordeaux, France

Master : Jean-Paul Cerri, Cryptologie, 24h TD, M1, Université de Bordeaux, France

Master : Jean-Paul Cerri, Arithmétique, 60h TD, M1, Université de Bordeaux, France

8.2.2. Supervision

PhD in progress : Ida Tucker, *Design of new advanced cryptosystems from homomorphic building blocks*, since October 2017, supervised by Guilhem Castagnos and Fabien Laguillaumie

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

PhD in progress: Jared Asuncion, *Class fields of complex multiplication fields*, since September 2017, supervised by A. Enge and Marco Streng (Universiteit Leiden).

PhD in progress: Chloë Martindale, *Isogeny graphs*, since 2013, supervised by A. Enge and Marco Streng (Universiteit Leiden).

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

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

PhD in progress: Antonin Riffaut *Calcul effectif de points spéciaux*, supervised by Y. Bilu and K. Belabas.

Master 2: Margarita Pierrakea, *Supersingular isogeny key-exchange*, supervised by D. Robert.

8.2.3. Juries

- A. Enge has written a report for the doctoral dissertation by Alexandre Le Meur, Université de Rennes, sur *Formules de Thomae généralisées à des courbes galoisiennes résolubles sur la droite projective*.
- A. Enge has written a report for the doctoral dissertation by Alexandre Gélin, Université Pierre et Marie Curie, *Class Group Computations in Number Fields and Applications to Cryptology*. K. Belabas was a member of the defense committee.
- K. Belabas has written a report for the doctoral dissertation of Thomas Camus, Université Grenoble-Alpes, *Méthodes algorithmiques pour les réseaux algébriques*.
- K. Belabas was a member of the defense committee of José Villanueva-Guttierez, Université de Bordeaux, *Sur quelques questions en théorie d'Iwasawa*.
- K. Belabas was a member of the defense committee of Philippe Moustrou, Université de Bordeaux, *Geometric distance graphs, lattices and polytopes*.
- J-M. Couveignes was a member of the defense committee of Carine Jaber (advisor Christian Klein), Université de Dijon, *Approche algorithmique au domaine fondamental de Siegel* the 28 June 2017.

- J-M. Couveignes was the president of the defense committee of Matthieu Rambaud (advisor Hugues Randriambololona), Telecom-ParisTech, *Shimura curves and bilinear multiplication algorithms in finite fields* the 2 September 2017.
- D. Robert is a member of the jury of Agregations de Mathematiques. He is also the codirector with Alain Couvreur of the option “calcul formel” of the Modelisation part of the oral examination.

8.3. Popularization

The book Guide to Pairing-Based Cryptography [26] has been published by CHAPMAN and HALL/CRC. D. Robert wrote with Sorina Ionica the chapter “Pairings” of this book. This book aims to help Engineers understand and implement pairing based cryptography; in the Chapter “Pairings”, D. Robert give a self contained definition and proof of the Weil and Tate pairing; including how to handle divisors with non disjoint support (this is often skipped in scientific papers but is important for practical implementations).

A. Page gave a popularization talk “À la découverte de la cryptologie : la science du secret” during the Fête de la Science event. Two groups of high school students and one group of Inria agents participated in this activity. Following this talk, three high school students decided to work on the RSA cryptosystem for their TPE essay and came back to the IMB to meet A. Page and talk about this topic in greater detail.

POLSYS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Emmanuel Prouff was a member of the organization committee of Eurocrypt 2017 (Paris, France, 2017, April 30 - May 4).

Jean-Charles Faugère and Ludovic Perret were members of the organization committee of the Quantum-Safe Cryptography for Industry (Paris, France, 2017, April 30).

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Mohab Safey El Din was PC Chair of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Kaiserslautern, Germany, 2017.

Jean-Charles Faugère was PC co-Chair of the International workshop on Parallel Symbolic Computation (PASCO), Kaiserslautern, Germany, 2017.

9.1.2.2. Member of the Conference Program Committees

Ludovic Perret was a member of the program-committee of

- 20th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC'17), Amsterdam, 28-31 March 2017

Emmanuel Prouff was a member of the steering committees of the following conferences

- Conference on Cryptographic Hardware and Embedded Systems 2017 (CHES 2017) (Taipei, Taiwan, 2017, Sept. 25-28);
- Smart Card Research and Advanced Application Conference (CARDIS 2017) (Lugano, Switzerland, 2017, Nov. 13-17).

Guénaël Renault was a member of the program committee of

- 7th Int'l Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2017;

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

- 7th Int'l Conference on Mathematical Aspects of Computer and Information Sciences (MACIS) 2017;
- 19th International Workshop on Computer Algebra in Scientific Computing (CASC) 2017.

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

- 11th International Workshop on Automated Deduction in Geometry (ADG 2016) (Strasbourg, France, June 27-29, 2016);
- 8th International Symposium on Symbolic Computation in Software Science (SCSS 2017) (Gammarth, Tunisia, 2017, April 6-9).

Dongming Wang was a member of the steering 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 an Associate Editor for:

- Designs, Codes and Cryptography (Springer, Berlin).
- The Computer Journal (Oxford University Press)
- Groups, Complexity, Cryptology (De Gruyter)

Emmanuel Prouff is an Associate Editor of the Journal of Cryptographic Engineering (Springer, Berlin).

Mohab Safey El Din is an Associate Editor of the 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 a plenary invited speaker at the

- SIAM Conference on Applied Algebraic Geometry, Atlanta (August 2017).

Ludovic Perret was invited speaker at the

- HEXATRUST Summer school 2017 (Paris, September 2017)

Emmanuel Prouff was invited speaker at the

- Journées du GDR-IM (Montpellier, France, 2017, Mar. 14-16).
- Aix-Marseille Cyber Security Forum (AMUSEC) (Marseille, France, 2017, Oct. 12-13).

Guénaël Renault was invited speaker at the

- Third French-Japanese Meeting on Cybersecurity (Tokyo, Japan, April 2017)

Mohab Safey El Din was invited speaker at:

- The mini-symposium on Euclidean Distance Degree at the 2017 SIAM Conference on Applied Algebraic Geometry, Atlanta, USA 2017;
- The math. seminar of the University of Dortmund, Germany;
- The Berlin-Leipzig Seminar on Algebra, Geometry and Combinatorics, Germany;
- The mini-symposium on Numeric and Symbolic Convex Programming for Polynomial Optimization, at the PGMO days, Saclay, France.

Dongming Wang invited speaker at the

- 7th International Conference on Mathematical Aspects of Computer and Information Sciences (Vienna, Austria, 2017, Nov. 15-17).
- 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (Timisoara, Romania, 2017, Sept. 21-24).
- 5th Summer School in Symbolic Computation (Nanning, China, 2017, July 16-22).

9.1.5. Scientific Expertise

Mohab Safey El Din was evaluator for the FWF International Program (Austrian funding agency).

Jean-Charles Faugère was the head of the hiring Committee for an associate professor in Grenoble.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Computation Modeling, 35 hours, M1, Université Pierre-et-Marie-Curie, France.

Master : In charge of Basics of Algebraic Algorithms, 73 hours, M1, Université Pierre-et-Marie-Curie & Polytech' UPMC, France.

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

Master : Projects supervision, 8 hours, M1, Université Pierre-et-Marie-Curie, France.

Licence : Introduction to Algorithmics, 40,5 hours, L2, Université Pierre-et-Marie-Curie, France.

Licence : Representations and Numerical Methods, 38,5 hours, L2, Université Pierre-et-Marie-Curie, France.

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

Jean-Charles Faugère had the following teaching activities:

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

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

Ludovic Perret is teaching a full service (192 hours), balanced between master and licence in cryptography, complexity and introduction to algorithms.

Mohab Safey El Din had the following teaching activities:

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

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

Master : In charge of the Security, Reliability and Numerical Efficiency Program in Master, 40 hours, M1 and M2, Université Pierre-et-Marie-Curie, France

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

9.2.2. Supervision

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

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

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

PhD in progress : Loïc Masure, Recognition and Side Channel Analysis, Emmanuel Prouff.

PhD in progress, Olive Chakraborty, Design and Analysis of Post-Quantum Schemes, started in May 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Nagardjun Chinthamani Dwarakanath, Design and Analysis of Fully Homomorphic Schemes, started in Dec. 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Solane El Hirch Design and Analysis of Post-Quantum Schemes, started in June 2017, Jean-Charles Faugère and Ludovic Perret.

PhD in progress, Xuan Vu. Algorithms for solving structured semi-algebraic systems, started in October 2017, Jean-Charles Faugère and Mohab Safey El Din.

9.2.3. Juries

Emmanuel Prouff was examiner in the PhD committee of N. Bruneau and M. Dugardin and in the HDR committees of J.-M. Dutertre and N. El Mrabet.

Guénaël Renault was referee in the Phd committee of T. Mefenza.

9.3. Popularization

The activity of POLSYS in post-quantum cryptography has been covered in several large audience magazines:

- “Enfin! La révolution quantique”, L’Usine Nouvelle, November 2017.
- “QUANTIQUE : THE NEXT BIG THING(K)”, L’Informaticien, November 2017.
- “L’ORDINATEUR QUANTIQUE VA-T-IL METTRE À MAL LA CYBERSÉCURITÉ MONDIALE?”, Bouygues Blog, October 2017.

Ludovic Perret is member of the Cloud Security Alliance (CSA) quantum-safe security working group. In particular, he contributed to the following documents:

- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. “Applied Quantum-Safe Security”, Feb. 2017.
- B. Huttner, J. Melia, G. Carter, L. Perret and L. Wilson. “Quantum Safe Security Glossary”, January 2017.

Ludovic Perret is also member of the quantum-safe cryptography specification group of the European Telecommunications Standards Institute (ETSI) where is the referee for a document on quantum-safe signatures.

Since May 2010, Daniel Lazard is engaged in a strong edition work on the English Wikipedia (more than 6 000 contributions, including vandalism revert and talk pages). Initially focused on the themes of POLSYS, these contributions were later enlarged to general algebra and algebraic geometry, because many elementary articles require to be expanded to be useful as a background for computer algebra. Examples of articles that have been subject of major editing: “System of polynomial equations” (created), “Computer algebra”, “Algebra”, “Algebraic geometry”, “Polynomial greatest common divisor”, “Polynomial factorization”, “Finite field”, “Hilbert series and Hilbert polynomial”,...

For the year 2017, this contribution amounts to about $2,000$ edits on the English Wikipedia.

Mohab Safey El Din was invited by FMJH to present and popularize symbolic and algebraic computation to Master students in Mathematics following the curricula proposed by Univ. Paris-Saclay.

SECRET Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- EuroS&P 2017: April 26-28, 2015, Paris (France): G. Leurent (poster chair);
- TQC 2017 (Theory of Quantum Computation, Communication and Cryptography): June 20-22, 2017, Paris (France): A. Chailloux, A. Leverrier.
- Dagstuhl Seminar 17401, "Quantum Cryptanalysis": October 1-6, 2017, Dagstuhl (Germany): N. Sendrier (co-organizer)
- Training School on Symmetric Cryptography and Blockchain: February 19-23, 2018, Torremolinos (Spain): A. Canteaut (co-organizer).

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

As a co-editor-in-chief of the journal *IACR Transactions on Symmetric Cryptology*, María Naya-Plasencia serves as a program chair of the conference *Fast Software Encryption (FSE)*, hold in Tokyo March 2017, and to be held in Bruges March 2018.

10.1.2.2. Member of the Conference Program Committees

- QIP 2017: January 16-20 2017, Seattle, USA (A. Chailloux, A. Leverrier);
- CT-RSA 2017: February 14-17, 2017, San Francisco, US (M. Naya-Plasencia);
- FSE 2017: March 5-8, 2017, Tokyo, Japan (A. Canteaut, G. Leurent, M. Naya-Plasencia);
- CryptoAction Symposium 2017: March 27-28, Amsterdam, the Netherlands (A. Canteaut);
- Financial Crypto 2017: April 3-7, 2017, Sliema, Malta (G. Leurent);
- Journées Codage et Cryptographie - C2 2017: April 23-28, La Bresse, France (G. Leurent);
- Eurocrypt 2017: 30 April- 4 May, 2017, Paris, France (M. Naya-Plasencia);
- Fq13: June 4-9, 2017, Gaeta, Italy (A. Canteaut);
- CEWQO 2017: June 26-30 2017, Lyngby, Denmark (A. Leverrier);
- PQCrypto 2017: 26-28 June, 2017, Utrecht, the Netherlands (M. Naya-Plasencia, N. Sendrier, J.P. Tillich)
- SAC 2017: August 16-18, 2017, Ottawa, Canada (G. Leurent, M. Naya-Plasencia);
- Crypto 2017: August 20-24, 2017, Santa Barbara, CA, USA (G. Leurent);
- AQIS 2017: September 4-8, 2017, Singapore (A. Chailloux);
- SCN 2018: September 5-7, 2018, Amalfi, Italy (G. Leurent);
- QCrypt 2017: 2017, September 18-22 2017, Cambridge, UK (A. Leverrier);
- WCC 2017: September 18-22, Saint-Petersburg, Russia (P. Charpin, J.-P. Tillich);
- FSE 2018: March 5-7, 2018, Bruges, Belgium (C. Boura, A. Canteaut, G. Leurent, M. Naya-Plasencia, L. Perrin);
- CryptoAction Symposium 2018: April 4-5, Sutomore, Montenegro (A. Canteaut);
- PQCrypto 2018: April 9-11, 2018, Fort Lauderdale, USA, (N. Sendrier, J.P. Tillich);

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editors: A. Canteaut, P. Charpin.
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut.
- *IACR Transactions on Symmetric Cryptology*, associate editors: C. Boura, A. Canteaut, G. Leurent, L. Perrin, co-editor-in-chief: M. Naya-Plasencia.
- *Annals of telecommunications*, associate editor: J.P. Tillich.
- *Advances in Mathematics for Communications*, associated editor : J.P. Tillich

10.1.3.2. Editor for books or special issues

- Special Issue on Coding and Cryptography, *Designs, Codes and Cryptography* : P. Charpin, T. Johansson, G. Kyureghyan, N. Sendrier and J.-P. Tillich, Eds., Volume 82, Issue 1-2, January 2017

10.1.3.3. Reviewer - Reviewing Activities

- Reviewer for Mathematical Reviews: P. Charpin.
- Reviewer for ERC proposals: G. Leurent

10.1.4. Invited Talks

- A. Leverrier, *Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction*, Trustworthy Quantum Information TyQi 2017, Paris, France, 19-21 June 2017.
- A. Leverrier, *Challenges in continuous-variable quantum cryptography*, QCRYPT 2017, Cambridge, UK, 18-22 September 2017.
- N. Sendrier, *Quantum Safe Cryptography from Codes: Present and Future*, 16th IMA International Conference on Cryptography and Coding, Oxford, UK, December 13, 2017.

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

- A. Canteaut, *Proving Resistance against Invariant Attacks: Properties of the Linear Layer* , Early Symmetric Crypto - ESC 2017, Canach, Luxembourg, January 2017
- A. Canteaut, *Proving resistance of a block cipher against invariant attacks*, BFA 2017 - Boolean Functions and their Applications, Os, Norway, July 2017.
- A. Chailloux, *A tight security reduction in the quantum random oracle model for code-based signature schemes*, IRIF Algocomp seminar, Paris, France, November 2017
- G. Leurent, *On the Practical (In-)Security of 64-bit Block Ciphers*, Early Symmetric Crypto - ESC 2017, Canach, Luxembourg, January 2017
- G. Leurent, *Breaking Symmetric Cryptosystems Using Quantum Algorithms*, Frontiers of Quantum Safe Cryptography - FOQUS, April 2017, Paris, France.
- G. Leurent, *Bad Symmetric Crypto in the Real World*, Journées Nationales 2017 Pré-GDR Sécurité Informatique, Paris, France, May 2017.
- A. Leverrier, *A Gaussian de Finetti theorem and application to truncations of random Haar matrices*, Workshop on "Probabilistic techniques and Quantum Information Theory", IHP, Paris, France, 23-27 October 2017.
- A. Leverrier, *Efficient decoding of random errors for quantum expander codes*, Conference on "Quantum Information Theory", IHP, Paris, France, 11-15 December 2017.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis* Dagstuhl seminar "Quantum Cryptanalysis", Dagstuhl, Germany, October 2017.

- N. Sendrier,*Code-based Cryptography*, PQCRYPTO Summer School on Post-Quantum Cryptography 2017, TU Eindhoven, June 2017. 5 hours.
- N. Sendrier,*Code-based Cryptography*, Executive School on Post-Quantum Cryptography 2017, TU Eindhoven, June 2017. 1 1/2 hours.
- J.P. Tillich *Décodage de codes LDPC quantiques*, Journées C2 La Bresse, April 27, 2017.
- J.P. Tillich *Code based cryptography and quantum attacks*, Dagstuhl seminar "Quantum Cryptanalysis", Dagstuhl, Germany, October 2017.
- J.P. Tillich *Recent advances in decoding quantum LDPC codes*, Recent advances in Quantum Computing, CEA Saclay, December 13, 2017.

10.1.5. Leadership within the Scientific Community

- A. Canteaut serves as a chair of the steering committee of *Fast Software Encryption (FSE)*.
- A. Canteaut serves on the steering committee of the international competition CAESAR for authenticated encryption [0].
- N. Sendrier serves on the steering committee of *Post-quantum cryptography (PQCrypto)*.
- N. Sendrier serves on the steering committee of the WCC conference series.
- N. Sendrier is a member of the “Comité de pilotage” of the ANR (défi 9).
- A. Leverrier serves on the steering committee of *DIM SIRTEQ* (réseau francilien pour les technologies quantiques).

10.1.6. Research Administration

- A. Canteaut serves as Head of Science of the Inria Paris research center since September 2017. She was deputy Head of Science from January to August 2017.
- A. Canteaut serves on the *Evaluation Committee* since September 2017.
- A. Canteaut was a member of the steering committee of the Fondation Sciences Mathématiques de Paris until June 2017.
- P. Charpin serves on the *Comité Parité* at Inria.
- M. Naya-Plasencia is a member of *Inria Paris CES Committee* (Comité de suivi doctoral).
- M. Naya-Plasencia is a member of *Inria Paris Scientific Hiring Committee* (Assignement of PhD, post-doctoral and delegation Inria fundings).
- M. Naya-Plasencia serves on the jury for PhD scholarships from EDITE.
- M. Naya-Plasencia serves on the *Comité des usagers du projet "rue Barrault"*.
- M. Naya-Plasencia serves on the *commission bureaux*.

10.1.7. Committees for the selection of professors, assistant professors and researchers

- Inria Paris Chargés de recherche: M. Naya-Plasencia
- Inria Directeurs de recherche: A. Canteaut
- Université Pierre-et-Marie-Curie, professor: A. Canteaut
- Université de Rouen, assistant professor: C. Boura, M. Naya-Plasencia
- Université de Limoges, assistant professor: C. Boura, M. Naya-Plasencia
- ENSEA, assistant Professor: M. Naya-Plasencia
- DTU Denmark, associate professor: A. Canteaut.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

[0] https://competitions.cr.yp.to/caesar.html

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

Master: A. Canteaut, *Symmetric crypography*, 6 hours M2, Ecole des Mines de Saint-Etienne, campus de Gardanne (ingénieurs Spécialité Microélectronique et Informatique), France, 2017.

Master: A. Chailloux, *Quantum Computing*, 9 hours, M2, University Paris-Diderot (MPRI), France;

Master: G. Leurent *Algorithmique et programmation*, 25 hours, M1, UVSQ, France;

Corps des Mines: G. Leurent *Cryptographie symétrique*, 9 hours, Telecom ParisTech, France;

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

10.2.2. Supervision

HdR : María Naya Plasencia, *Symmetric Cryptography for Long-Term Security*, University Pierre-et-Marie-Curie, May 5, 2017.

HdR : Anthony Leverrier, *Protecting information in a quantum world: from cryptography to error correction*, University Pierre-et-Marie-Curie, September 27, 2017.

PhD : Julia Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, University Pierre-et-Marie-Curie, March 20, 2017.

PhD : Kaushik Chakraborty, *Cryptography with spacetime constraints*, Université Pierre-et-Marie Curie, October 12, 2017.

PhD : Adrien Hauteville, *Nouveaux protocoles et nouvelles attaques pour la cryptologie basée sur les codes en métrique rang* , University of Limoges, December 4, 2017.

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

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

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

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

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

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

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

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

PhD in progress: Matthieu Lequesne, *Attaques par canaux cachés sur les cryptosystèmes à base de codes MDPC quasi-cycliques*, since September 2017, supervisor: N. Sendrier

PhD in progress: Ferdinand Sibleyras, *Security of modes of operation*, since October 2017, supervisor: G. Leurent and A. Canteaut

PhD in progress: Valentin Vasseur, *Etude du décodage des codes QC-MDPC*, since October 2017, supervisor: N. Sendrier

PhD in progress: Rémi Bricout, *Etude de scénarios non-locaux quantiques à l'aide d'outils de la théorie de l'information quantique*, since September 2017, supervisor: A. Chailloux and A. Leverrier

PhD in progress: Shouvik Ghorai, *Beyond-QKD continuous-variable quantum cryptographic protocols*, since October 2017, supervisors: E. Diamanti (UPMC), A. Leverrier

PhD in progress: Andrea Olivo, *Partir de contraintes relativistes pour faire de la cryptographie quantique*, since November 2017, supervisors: A. Chailloux and F. Grosshans (laboratoire Aimé Cotton).

10.2.3. Juries

- C. Mavromati, *Cryptanalyse des algorithmes de type Even-Mansour*, University Paris-Saclay, January 24, 2017, committee: A. Canteaut (reviewer).
- J. Chaulet, *Study of public-key cryptosystems based on MDPC quasi-cyclic codes*, University Pierre-et-Marie-Curie, March 20, 2017, committee: N. Sendrier (supervisor), JP Tillich.
- R. do Canto de Loura, *Quantum measures, noise and measurement errors in a quantum bit commitment protocol*, Universidade de Lisboa, Instituto Superior Tecnico, March 31, 2017, committee: A. Leverrier (reviewer).
- M. Naya-Plasencia, *Symmetric Cryptography for Long-Term Security*, Habilitation, University Pierre-et-Marie-Curie, May 5, 2017, committee: A. Canteaut.
- H. Kalachi, *Sécurité de Protocoles Cryptographiques Fondés sur la Théorie des Codes Correcteurs d'Erreurs*, July 5, 2017, University of Rouen, committee: J.P. Tillich;
- B. Dravie, *Synchronisation et systèmes dynamiques, application à la cryptographie*, University of Lorraine, July 6, 2017, committee: A. Canteaut (reviewer).
- V. Dragoi, *Approche algébrique pour l'étude et la résolution de problèmes algorithmiques issus de la cryptographie et de la théorie des codes*, July 6, 2017, University of Rouen, committee: N. Sendrier (reviewer), J.P. Tillich;
- V. Migliore, *Cybersécurité matérielle et conception de composants dédiés au calcul homomorphe*, Université de Bretagne Sud, September 26, 2017. committee: N. Sendrier (reviewer);
- A. Leverrier, *Protecting information in a quantum world: from cryptography to error correction*, Habilitation, University Pierre-et-Marie-Curie, September 27, 2017, committee: J.P. Tillich;
- A. Bannier, *Combinatorial analysis of block ciphers with trapdoor*, Arts et Métiers ParisTech, September 29, 2017, committee: A. Canteaut;
- K. Chakraborty, *Cryptography with spacetime constraints*, Université Pierre-et-Marie Curie, October 12, 2017, committee: A. Leverrier (supervisor), J.P. Tillich (supervisor);
- A. Hauteville, *Nouveaux protocoles et nouvelles attaques pour la cryptologie basée sur les codes en métrique rang* , University of Limoges, December 4, 2017, committee: N. Sendrier, J.P. Tillich (supervisor);
- D. Mirandola, *On products of linear error correcting codes*, Leiden University, the Netherlands, and Univ. de Bordeaux, December 6, 2017, committee: A. Canteaut (reviewer, chair).
- G. Spini, *Unconditionally secure cryptographic protocols from coding-theoretic primitives*, Leiden University, the Netherlands, and Univ. de Bordeaux, December 6, 2017, committee: A. Canteaut (chair).
- P. Méaux, *Chiffrement complètement homomorphe hybride*, Research University PSL, December 8, 2017, committee: A. Canteaut (reviewer);
- M. Saad Taha. *Algebraic Approach for Code Equivalence*, Université de Rouen, December 18, 2017. committee: N. Sendrier (reviewer), J.P. Tillich;

10.3. Popularization

- **Alkindi cipher challenge:** Several members of the project-team are involved in the cipher challenge for high-school students "concours Alkindi" http://www.concours-alkindi.fr/. Matthieu Lequesne organized the challenge and created the scientific content of the competition. He also gave a talk during the final of the cipher challege Alkindi on May 17 at the "Cité des Sciences" in Paris. The 2018 edition of the competition has been launched in December 2017 at Lycée de la Vallée de Chevreuse, Gif-sur-Yvette. Matthieu Lequesne, Sébastien Duval and Yann Rotella gave talks on cryptography during the opening ceremony. The best teams from Académies de Dijon and Orléans-Tours have been visiting the SECRET project-team in June 2017 https://www.youtube.com/watch?v=EVLHEOWAORc.
- N. Sendrier, *Code-Based Cryptography: State of the Art and Perspectives*, IEEE Security & Privacy, Special Issue on Post-quantum Cryptography. July/August 2017.
- A. Chailloux *Cryptographie Quantique en théorie* - Journée Maths en Mouvement sur l'ordinateur quantique organized by the FSMP, Paris, France, May 2017
- Matthieu Lequesne co-organized the final of the French Tournament of Young Mathematicians at École polytechnique on May 26-28 and was chaired the jury sessions. He also participated to the elaboration of the problems for the 8th French Tournament of Young Mathematicians (TFJM^2) in December 2017.
- Matthieu Lequesne co-organized the International Tournament of Young Mathematicians (ITYM) in Iasi, Romania in July 2017 and was part of the international jury.
- Matthieu Lequesne taught for one week during a mathematical summer camp for high school students in Bethlehem, Palestine, organized by the Al Khwarizmi Noether Institute in August 2017.
- Matthieu Lequesne co-organized a weekend for female high-school students interested in mathematics (Rendez-vous des Jeunes Mathématiciennes) at ENS Ulm, November 25-26.
- Yann Rotella gave a talk on cryptography at Lycée Théophile Gautier, Tarbes, January 31, 2017.
- Yann Rotella gave a presentation for *Raconte-moi ta thèse !* during Fete de la Science, at IHP, Paris, October 2017.
- Several members of the team (C. Boura, A. Canteaut, M. Lequesne, A. Leverrier, Y. Rotella) have been involved in the *Cinquante ans d'Inria*, November 2017. They hold a stand to present a serious game on cryptography. A. Canteaut has participated on a panel on Cyber-security. A. Leverrier gave a short talk (pitch de science) on quantum computing.
- Matthieu Lequesne was auditioned by the committee in charge of proposing a reform of mathematical education (Mission Maths Villani-Torossian) on November 29.

SPECFUN Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

- Alin Bostan is part of the Scientific advisory board of the conference series *Effective Methods in Algebraic Geometry* (MEGA).
- Frédéric Chyzak is member of the steering committee of the *Journées Nationales de Calcul Formel* (JNCF), the annual meeting of the French computer algebra community.
- Frédéric Chyzak is elected member of the steering committee of the *International Symposium on Symbolic and Algebraic Computation* (ISSAC, 3-year term, 2016–2018).
- Assia Mahboubi has served on the scientific committee of the Journées Scientifiques Inria and of the EUTypes summer school.

8.1.1.2. Member of the Organizing Committees

- Georges Gonthier was co-chair or the organising committee of the Big Proof thematic program held at the Newton Institute (Cambridge, UK) in June-August 2017.
- Assia Mahboubi has organized the TTT workshop, satellite of the POPL'17 conference.

8.1.1.3. Other

The team organizes a regular seminar[0], with roughly 15–20 talks a year. The topics reflect the team's interests: computer algebra, combinatorics, number theory, formal proofs, and related domains.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

- Assia Mahboubi has served as member of the conference program committees of the international conferences CPP 17, CADE 17, ITP 17, and on the program committee of the international workshops TYPES 17, TyDe 17, HoTT/UF 17.

8.1.2.2. Reviewer

- Alin Bostan has served as reviewer for the selection of the international conferences ISSAC 2017 and MEGA 2017.
- Frédéric Chyzak has served as reviewer for the selection of the international conference ISSAC 2017.
- Assia Mahboubi has served as external reviewer for the international conference LICS 17.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

- Georges Gonthier is on the editorial board of the Journal of Formalized Reasoning.

8.1.3.2. Reviewer - Reviewing Activities

- Alin Bostan has served as a reviewer for the journals: *Journal of Symbolic Computation*; *Linear Algebra and its Applications*; *Journal of Algebra and its Applications*; *Journal of Complexity*; *Advances in Applied Mathematics*; *Journal of Combinatorial Theory, Series A*.

[0] https://specfun.inria.fr/seminar/

- Assia Mahboubi has served as reviewer for the journals: *Annals of Mathematics and Artificial Intelligence*; *Journal of Automated Reasoning*.

8.1.4. Invited Talks

- Alin Bostan has been invited to give a series of three lectures at the *JNCF – Journées Nationales de Calcul Formel* (CIRM, Luminy, France), January 16–18, 2017, http://jncf2017.lip6.fr.
- Alin Bostan has been invited to give a talk at the workshop *EDATE – Equations différentielles : aspects théoriques et effectifs*, Grenoble, March 13–15, 2017, http://edate2017.sciencesconf.org/.
- Alin Bostan has been invited to give a talk at the workshop *ANT – Automata in Number Theory*, île de Porquerolles, May 30—June 2, 2017, http://indico.math.cnrs.fr/event/2347/.
- Alin Bostan has been invited to give a talk at the workshop *Lattice walks at the Interface of Algebra, Analysis and Combinatorics*, BIRS, Banff, Canada, September 17—22, 2017, http://www.birs.ca/events/2017/5-day-workshops/17w5090.
- Alin Bostan has been invited to give a series of introductory lectures at the *Workshop on Computer Algebra in Combinatorics*, Erwin Schrödinger Institut (ESI), Vienna, Austria, November 13–17, 2017, http://www.mat.univie.ac.at/~kratt/esi4/workshop2.html.
- Frédéric Chyzak has been invited to give a talk at the *Second International Conference "Computer Algebra in Moscow"*, Plekhanov Russian University of Economics, Moscow, Russia, October 30 to November 30, 2017, http://www.ccas.ru/ca/conference.
- Frédéric Chyzak has been invited to give a talk at the *Workshop on Computer Algebra in Combinatorics*, Erwin Schrödinger Institut (ESI), Vienna, Austria, November 13–17, 2017, http://www.mat.univie.ac.at/~kratt/esi4/workshop2.html.
- Georges Gonthier gave an invited talk at the Special Session on Computer-Aided Proofs of the *Association for Symbolic Logic 2017 North American Meeting*, Boise, Idaho, USA, March 20–23, 2017.
- Georges Gonthier gave an invited talk at the *Second Conference on Artificial Intelligence and Theorem Proving (AITP'17)*, Obergürgl, Austria, March 26–30, 2017.
- Georges Gonthier gave a talk at the *ERCIM Workshop on Blockchains*, Paris, May 23, 2017.
- Georges Gonthier gave an invited talk at the Workshop *Computer-aided Mathematical Proof*, part of the Big Proof Program, Isaac Newton Institute, Cambridge, U.K.
- Pierre Lairez gave an invited talk at *Effective Methods in Algebraic Geometry (MEGGA 2017)*, Nice.
- Pierre Lairez gave an invited talk at the *Conference on Foundations of Computational Mathematics (FoCM 2017)*, Barcelona, Spain.
- Assia Mahboubi has been invited to give a talk at the General Mathematics Colloquium of the VU Amsterdam, The Netherlands.
- Assia Mahboubi has been invited to give a talk at the Workshop *Computer-aided Mathematical Proof*, part of the Big Proof Program, Isaac Newton Institute, Cambridge, U.K.

8.1.5. Leadership within the Scientific Community

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

8.1.6. Research Administration

- Georges Gonthier serves on the Conseil de l'École Doctorale de Mathématiques Hadamard.
- Assia Mahboubi has been a member of the *Commission Scientifique* of Inria Saclay — Île-de-France, until September 2017.

8.2. Teaching - Supervision - Juries

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

8.2.1. Teaching

Licence:

Thomas Sibut-Pinote, *Les bases de la programmation et de l'algorithmique*, 32h, L3, École polytechnique, France.

Thomas Sibut-Pinote, *Les principes des langages de programmation*, 32h, L3, École polytechnique, France.

Master:

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

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

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

Assia Mahboubi, *Algorithmes d'élimination des quantificateurs*, 3h, M2, Université Rennes 1, France.

8.2.2. Supervision

HdR : Alin Bostan, *Computer algebra for lattice path combinatorics* [1], Université Paris 13, December 15, 2017.

PhD : Thomas Sibut-Pinote, *Investigations en Mathématiques Assistées par Ordinateur: Expérimentation, Calcul et Certification*, Université Paris-Saclay, December 4, 2017.

8.2.3. Juries

- Frédéric Chyzak has served as an examiner in the PhD jury of Cyril Hugounenq *Volcans et calcul d'isogénies*, Université de Versailles – Saint-Quentin-en-Yvelines, September 25, 2017.
- Frédéric Chyzak has been a member of the hiring jury at Inria (Concours CR 2017).
- Georges Gonthier served on the Habilitation à diriger des Recherches of Paul-André Melliès *Une étude micrologique de la négation*, Université Paris Diderot, November 20, 2017.
- Assia Mahboubi has been a member of the hiring jury at Inria (Concours CR 2017).
- Assia Mahboubi has served as an examiner in the PhD jury of Evmorfia-Iro Bartzia *Une formalisation des courbes elliptiques pour la cryptographie*, Université Paris-Saclay, February 15, 2017.
- Assia Mahboubi has served as an examiner in the PhD jury of Étienne Miquey *Réalisabilité classique et effets de bord*, Université Paris Diderot, November 17, 2017.
- Assia Mahboubi has been a member of the hiring jury of a Maître de conférence position at Université Paris Diderot.

8.3. Popularization

- Assia Mahboubi has written an article for the MathExpress journal, at the occasion of the *salon Culture & Jeux Mathématiques*. See the Maths Language express volume at http://www.cijm.org/accueil/productions-cijm/90-maths-express.

CAIRN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Chair of Conference Program Committees

- O. Sentieys was Track Chair at IEEE NEWCAS.

9.1.2. 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.
- S. Derrien was a member of technical program committee of IEEE FPL and ARC conferences and of WRC and Impact workshops.
- O. Sentieys was a member of technical program committee of IEEE/ACM DATE, IEEE FPL, ACM ENSSys, ACM SBCCI, IEEE ReConFig, FPGA4GPC.

9.1.3. Member of the Editorial Boards of Journals

- D. Chillet is member of the Editor Board of Journal of Real-Time Image Processing (JRTIP).
- O. Sentieys is member of the editorial board of Journal of Low Power Electronics and International Journal of Distributed Sensor Networks.

9.1.4. Invited Talks

- O. Sentieys gave an invited talk at FETCH (École d’hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Mont Tremblant, Canada, January 2017 on “Need more Energy Efficiency? Agree to Compute Inexactly”.
- O. Sentieys gave an invited talk at GDR SoC^2, Paris, France, November 2017 on “Controlling Inexact Computations at Compile Time and Runtime”.
- O. Sentieys gave an invited talk at IoT2Sustain Workshop, London, UK, July 2017 on “Challenges in Energy Efficiency of Computing Architectures: from Sensors to Clouds”.
- O. Sentieys gave an invited course at ARCHI Spring School, Nancy, France, March 2017 on “Design of VLSI Integrated Circuits – A (very) deep dive into processors”.

9.1.5. Leadership within the Scientific Community

- D. Chillet is member of the Board of Directors of Gretsi Association.
- D. Chillet is co-animator of the topics "Connected Objects" and "Near Sensor Computing" of GDR SoC^2.
- F. Charot and O. Sentieys are members of the steering committee of a CNRS Spring School for graduate students on embedded systems architectures and associated design tools (ARCHI).
- C. Killian was Co-Organizer of the Thematic Day on "Emerging Interconnect Technologies in Many Core Architectures" of GDR SoC^2, November 27, 2017.
- O. Sentieys is a member of the steering committee of a CNRS spring school for graduate students on low-power design (ECOFAC).
- O. Sentieys is a member of the steering committee of GDR SoC^2.

9.1.6. Scientific Expertise

- E. Casseau served as an expert for the Natural Sciences and Engineering Research Council of Canada (NSERC), program Discovery Grant 2017.
- O. Sentieys served as a jury member in the EDAA Outstanding Dissertations Award (ODA).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

E. Casseau: signal processing, 16h, ENSSAT (L3)
E. Casseau: low power design, 6h, ENSSAT (M1)
E. Casseau: real time design methodology, 24h, ENSSAT (M1)
E. Casseau: computer architecture, 24h, ENSSAT (M1)
E. Casseau: SoC and high-level synthesis, 24h, Master by Research (SISEA) and ENSSAT (M2)
S. Derrien: component and system synthesis, 20h, Master by Research (ISTIC) (M2)
S. Derrien: computer architecture, 12h, ENS Rennes (L3)
S. Derrien: computer architecture, 24h, ISTIC (L3)
S. Derrien: introduction to operating systems, 8h, ISTIC (M1)
S. Derrien: embedded architectures, 48h, ISTIC (M1)
S. Derrien: high-level synthesis, 6h, ISTIC (M1)
S. Derrien: software engineering project, 40h, ISTIC (M1)
F. Charot: processor architecture, 25h, Univ. of Science and Tech. of Hanoi (M1)
D. Chillet: embedded processor architecture, 20h, ENSSAT (M1)
D. Chillet: multimedia processor architectures, 24h, ENSSAT (M2)
D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne (M2)
C. Killian: digital electronics, 62h, IUT Lannion (L1)
C. Killian: signal processing, 36h, IUT Lannion (L2)
C. Killian: automated measurements, 56h, IUT Lannion (L2)
C. Killian: measurement chain, 58h, IUT Lannion (L2)
C. Killian: embedded systems programming, 12h, IUT Lannion (L2)
C. Killian: automatic control, 18h, IUT Lannion (L2)
A. Kritikakou: computer architecture 1, 32h, ISTIC (L3)
A. Kritikakou: computer architecture 2, 44h, ISTIC (L3)
A. Kritikakou: C and unix programming languages, 102h, ISTIC (L3)
A. Kritikakou: operating systems, 96h, ISTIC (L3)
A. Kritikakou: multitasking operating systems, 20h, ISTIC (M1)
O. Sentieys: digital signal processing, 40h, ENSSAT (M1)
O. Sentieys: VLSI integrated circuit design, 40h, ENSSAT (M1)
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 (ISTIC) (M2)

9.2.2. Teaching Responsibilities

- C. Wolinski is the Director of ESIR.
- S. Derrien was the responsible of the first year (M1) of the Master of Computer Science at ISTIC until Aug. 2017.
- O. Sentieys is responsible of the ”Embedded Systems” major of the SISEA Master by Research.
- D. Chillet is the responsible of the ICT Master of University of Science and Technology of Hanoi.
- C. Killian is the responsible of the second year of the Physical Measurement DUT at IUT of Lannion.

ENSSAT stands for *”École Nationale Supérieure des Sciences Appliquées et de Technologie”* and is an *”École d'Ingénieurs”* of the University of Rennes 1, located in Lannion.

ISTIC is the Electrical Engineering and Computer Science Department of the University of Rennes 1.
ESIR stands for *"École supérieure d'ingénieur de Rennes"* and is an *"École d'Ingénieurs"* of the University of Rennes 1, located in Rennes.

9.2.3. Supervision

PhD: Benjamin Barrois, Methods to Evaluate Accuracy-Energy Trade-Off in Operator-Level Approximate Computing, Dec. 2017, O. Sentieys.

PhD: Gaël Deest, Implementation Trade-Offs for FPGA Accelerators, Dec. 2017, S. Derrien.

PhD: Xuan Chien Le, Improving performance of non-intrusive load monitoring with low-cost sensor networks, Apr. 2017, O. Sentieys, B. Vrigneau.

PhD: Rengarajan Ragavan, Error handling and energy estimation for error resilient near-threshold computing, Sep. 2017, O. Sentieys, C. Killian.

PhD: Baptiste Roux, Methodology and Tools for Energy-aware Task Mapping on Heterogeneous Multiprocessor Architectures, Nov. 2017, O. Sentieys, M. Gautier.

PhD in progress: Minh Thanh Cong, Hardware Accelerated Simulation of Heterogeneous Multicore Platforms, May 2017, F. Charot, S. Derrien.

PhD in progress: Petr Dobias, Towards efficient application execution on resilient multi-core architectures, Oct. 2017, E. Casseau.

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

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

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

PhD in progress: Van-Phu Ha, Application-Level Tuning of Accuracy, Nov. 2017, T. Yuki, O. Sentieys.

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

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

PhD in progress: Thibaut Marty, Compiler support for speculative custom hardware accelerators, Sep. 2017, T. Yuki, O. Sentieys.

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

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

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

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

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

CAMUS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Selection

10.1.1.1. Member of the Conference Program Committees

Philippe Clauss and Cédric Bastoul have been part of the program committee of IMPACT 2017 and 2018 (International Workshop on Polyhedral Compilation Techniques), held in conjunction with the international conference HiPEAC.

Cédric Bastoul has been part of the program committee of the international conference on Compiler Construction 2017 and 2018 (CC'2017 and CC'2018).

Cédric Bastoul and Vincent Loechner have been part of the program committee of the HIP3ES workshop 2017 and 2018 (International Workshop on High Performance Energy Efficient Embedded Systems), co-organized by Cédric Bastoul in conjunction with the international conference HiPEAC.

Arthur Charguéraud has been part of the program committee for the Conference on Verified Software: Theories, Tools, and Experiments (VSTTE 2017).

10.1.1.2. Reviewer

Philippe Clauss has been reviewer for the following conferences and workshops: IMPACT 2017 and 2018 (International Workshop on Polyhedral Compilation Techniques), CC 2017 (International Conference on Compiler Construction).

Cédric Bastoul has been reviewer for the following international conferences and workshops: CC 2017 and 2018 (International Conference on Compiler Construction), PARMA 2017 (International Workshop on Parallel Programming and Run-Time Management Techniques for Many-core Architectures), IMPACT 2017 and 2018 (International Workshop on Polyhedral Compilation Techniques), HIP3ES 2017 and 2018 (International Workshop on High Performance Energy Efficient Embedded Systems).

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

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

10.1.2.2. Reviewer - Reviewing Activities

Philippe Clauss has been reviewer for the following journals: Journal of Computer and System Sciences, Journal of Software: Practice and Experience, IEEE Transactions on Computers.

Cédric Bastoul has been reviewer for the following journals: Journal of Parallel, Emergent and Distributed Systems, and IEEE Transactions on Computers.

Arthur Charguéraud has been reviewer for JAR (Journal of Automated Reasoning), DMTCS (journal of Discrete Mathematics and Theoretical Computer Science), and JFP (Journal of Functional Programming).

Vincent Loechner has been reviewer for: JAR (Journal of Automated Reasoning, Springer), STTT (Int. J. on Software Tools for Technology Transfer, Springer), ComCom (Computer Communications, Elsevier).

10.1.3. Invited Talks

Philippe Clauss has been invited to give a talk at a seminar dedicated to Jean-Luc Gaudiot, organized by the French Computer Science Engineering school ENSIEE, Paris, September the 21st 2017. The topic of his talk was: *Le modèle polyédrique au delà de la compilation statique, des fonctions affines et des boucles*.

Arthur Charguéraud has been invited to give a talk at ENS Rennes, on November 21st, 2017, to present the CFML interactive program verification tool.

10.1.4. Scientific Expertise

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

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 and serves as co-editor of the standards document. 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.

In 2017, he was the one of the main forces behind the elaboration of C17, the new version of the C standard that is expected to go into ballot in the member states end of 2017.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

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

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

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

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

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

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

Master : Jens Gustedt, parallélisme, 14h, M1, Université de Strasbourg, France

IUT d'Informatique : Alain Ketterlin, Architecture et programmation des mécanismes de base d'un système informatique, 68h, Université de Strasbourg, France

Licence : Alain Ketterlin, Algorithmique et programmation L1, 82h, Université de Strasbourg, France

Master (Informatique) : Alain Ketterlin, Ingénierie de la preuve en Coq, 18h, Université de Strasbourg, France

Master (Calcul Scientifique et Mathématiques de l'Information) : Alain Ketterlin, Compilation et optimisation, 26h, Université de Strasbourg, France

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

Licence : Cédric Bastoul, Concurrent Systems, 20h, L3, Université de Strasbourg, France

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

Master : Cédric Bastoul, Parallelism, 19h, M1, Université de Strasbourg, France

Master : Cédric Bastoul, Introduction to Research, 11h, L2+M1, Université de Strasbourg, France

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

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

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

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

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

Licence : Eric Violard, Systèmes Concurrents (licence informatique), 7h eq. TD, L3, Université de Strasbourg, France

Master : Arthur Charguéraud, Proof of Programs (MPRI), 12h, M2, Université Paris Diderot, France

Licence : Vincent Loechner, responsable pédagogique de la licence professionnelle SIL spécialité ARS (Administration de Réseaux et Services), 24h, L3, université de Strasbourg, France

Licence : Vincent Loechner, systèmes d'exploitation, 13h, L2, université de Strasbourg, France

Licence : Vincent Loechner, administration système et internet, 54h, L3, université de Strasbourg, France

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

Master : Vincent Loechner, OS embarqués, 34h, M2, université de Strasbourg, France

Master : Vincent Loechner, calcul parallèle, 30h, 3ième année école d'ingénieur (TPS), université de Strasbourg, France

10.2.2. Supervision

PhD: Nabil Hallou, *Dynamic binary optimizations*, University of Rennes, December the 18th 2017, Erven Rohou (PACAP team) and Philippe Clauss

PhD in progress: Salwa Kobeissi, *Dynamic parallelization of recursive functions by transformation into loops*, September 2017, Philippe Clauss

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: Yann Barsamian, *Optimization and parallelization of particle and semi-Lagrangian methods for multi species plasma simulations*, since Oct 2014, Eric Violard.

PhD in progress: Armaël Géneau, *Formal verification of complexity analyses*, since Sept 2016, co-advised by Arthur Charguéraud and François Pottier, from team Gallium (Inria Paris), where Armaël is located.

PhD in progress: Harenome Ranaivoarivony-Razanajato, *Hierarchical Parallelization and Optimization*, Oct. 2016, Cédric Bastoul and Vincent Loechner

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

PhD in progress : Paul Godard, *Parallelization and Scalability of a Graphical Pipeline for Professionnal Inkjet Printing*, Jun. 2016, Cédric Bastoul and Vincent Loechner

10.2.3. Juries

Philippe Clauss participated to the following PhD committees in 2017:

Date	**Candidate**	**Place**	**Role**
Dec. 11	Alexandre Maréchal	Université de Grenoble	Examiner
Dec. 18	Nabil Hallou	Université de Rennes	Co-advisor
Dec. 21	Jordy Ruiz	Université de Toulouse	Reviewer

Vincent Loechner participated as examiner to the PhD committee of Maroua Maalej, defended on Sept. 26th 2017 at Université Claude Bernard (Lyon 1).

10.3. Popularization

A. Charguéraud is one of the three organizers of the *Concours Castor informatique*http://castor-informatique.fr/. The purpose of the Concours Castor in to introduce pupils (from *CM1* to *Terminale*) to computer sciences. More than 500,000 teenagers played with the interactive exercises in November 2017.

Jens Gustedt is 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.

Cédric Bastoul prepared activities and participated to *Fête de la Science* at University of Strasbourg in October 2017.

CORSE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Fabrice Rastello: General Chair "Journées française de la compilation", Lyon, June 2017

9.1.1.2. Member of the Organizing Committees

- Fabrice Rastello: Steering Committee ACM/IEEE CGO; Steering Committee "Journées française de la compilation"
- Yliès Falcone: Publicity Chair of the 24th International SPIN Symposium on Model Checking of Software

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Fabrice Rastello: Program Chair "Journées française de la compilation", Lyon, June 2017
- Yliès Falcone: Track Chair on Software Verification and Testing at the 2017 ACM Symposium on Applied Computing

9.1.2.2. Member of the Conference Program Committees

- Fabrice Rastello: ACM/IEEE CGO'18
- François Broquedis: IEEE IPDPS'18
- Jean-François Méhaut: IEEE IPDPS'18
- Frédéric Desprez: ACM/SIGSIM HPC'17, ACM/SIGARCH HPDC'17, IEEE/ACM ISFEC'17, IEEE IPDS'17, IEEE ICDCS'17, IEEE ICA3PP'17, Special Track: Vision/Blue Sky Thinking, EBDMA'17, Europar'17, ICPADS'17, Closer 2017
- Yliès Falcone: CRI'17, MSR'17, RV-CuBES, RV'17, RW-BRMS'17, TASE 2017, iFM 2017, PDP 2017, DATE 2017 – Topic E3

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing activities

- Frédéric Desprez: IJHPCA
- Yliès Falcone: ACM Transactions on Software Engineering and Methodology (TOSEM), Formal Aspects of Computing, ACM Transactions on Automatic and Control, Acta Informatica, Formal Methods in System Design

9.1.4. Invited talks

- Frédéric Desprez: Entretiens Jacques Cartier, Montréal, Oct. 18 2017 "From IoT Devices to Cloud Computing Infrastructures"

9.1.5. Scientific expertise

- Frédéric Desprez: European project in the FP7 framework; Comité d'orientation stratégique de CIRRUS (COMUE Paris); Groupe Technique GENCI; GENCI, expert for grants of computing resources (CT6); COFECUB - CAPES 2018.
- Yliès Falcone: Representative of France in the COST Action ARVI

- Yliès Falcone: COST Action ARVI, co-leader of Working Group on Core Run-Time Verification
- Jean-François Méhaut: Eurolab-4-HPC, expert for cross site mobility research grants
- Jean-François Méhaut: GENCI, expert for grants of computing resources (CT6)
- Jean-François Méhaut: GENCI, reviewer for C3I (*Certificat de Compétences en Calcul Intensif*)

9.1.6. Research administration

- Frédéric Desprez: Deputy Scientific Director at INRIA
- Frédéric Desprez: Director of the GIS GRID5000
- Frédéric Desprez: Conseil Scientifique ESIEE Paris
- Yliès Falcone: Mission Valorisation for Laboratoire d'Informatique de Grenoble

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

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

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

Master I: Jean-François Méhaut, Parallel Algorithms and Programming, 10 hours (M1 Informatique), UFR IM2AG, Université Grenoble Alpes

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

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

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

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

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

Master: Florent Bouchez Tichadou, Compilation project, 20 hours, M1 Info & M1 MoSIG

Licence: Florent Bouchez Tichadou, C programming, 20 hours, L3, Grenoble Institute of Technology (Ensimag)

Licence: Florent Bouchez Tichadou, Introduction to Programming, 24 hours, L1 UGA

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

Licence: Florent Bouchez Tichadou, Algorithms languages and programming, 111 hours, L2 UGA

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

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

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

Master I: Yliès Falcone Programming Language Semantics and Compiler Design, MoSIG and Master informatique, 96 hours

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

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

Master I: Frédéric Desprez, Parallel Algorithms and Programming, 30 hours (MOSIG and Info)

9.2.2. Supervision

PhD defended: Thomas Gonçalves, Contributions à la parallélisation de méthodes de type transport Monte-Carlo, defended on September 28 2017, advised by Marc Perache (CEA/DAM), Frédéric Desprez, and Jean-François Méhaut

PhD defended: Vanessa Vargas, Approche logicielle pour améliorer la fiabilité d'applications parallèles implémentées sur des processeurs multi-cœurs et many-cœurs, defended on April 28 2017, advised by Raoul Velazco (CNRS, TIMA), and Jean-François Méhaut

PhD defended: Hosein Nazarpour, Monitoring Distributed and Multi-threaded Component-Based Systems, defended on June 26, 2017, advised by Yliès Falcone and Saddek Bensalem (Verimag).

PhD defended: Matthieu Renard, Run-Time Enforcement of (Timed) Properties with Uncontrollable Events, defended on December 11, 2017, advised by Yliès Falcone, Antoine Rollet and Mohamed Mosbah (University of Bordeaux).

PhD defended: Pedro Silva, On the mapping of distributed applications on multiple clouds, defended on December 11 2017, advised by Frederic Desprez, C. Perez (INRIA, Avalon team)

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: Antoine El-Hokayem, Decentralised and Distributed Monitoring of Cyber-Physical Systems, October 2017, advised by Yliès Falcone.

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

PhD in progress: Georgios Christodoulis, Adaptation of a heterogeneous run-time system to efficiently exploit FPGA, October 2015, advised by Frederic Desprez, Olivier Muller (TIMA/SLS), and François Broquedis

PhD in progress: Luis Felipe Millani, Auto-tuning for optimizations of performance and power consumption, November 2015, advised by Lucas Schnoor (UFRGS) and Jean-François Méhaut

PhD in progress: Philippe Virouleau, Improving the performance of task-based run-time systems on large scale NUMA machines, March 2015, advised by Thierry Gautier (INRIA/AVALON), Fabrice Rastello, and François Broquedis

PhD in progress: Raphaël Jakse, Monitoring and Debugging Component-Based Systems, October 2016, advised by Jean-François Méhaut and Yliès Falcone.

PhD in progress: Thomas Messi Nguelé, Domain Specific Languages for Social Networks Analysis on Multi-Core Architectures, October 2014, advised by Maurice Tchuenté (Yaoundé I, LIRIMA) and Jean-François Méhaut

PhD in progress: Ye Xia, Scaling and placement for autonomic management of elasticity of applications in a widely distributed cloud, November 2015, advised by Thierry Coupaye (Orange), Frédéric Desprez, and Xavier Etchevers (Orange)

PhD in progress: Pedro Henrique Penna, Towards an Operating System for Manycore Platforms, October 2017, advised by Marcio Castro (UFSC), François Broquedis, Henrique Cota de Freitas (PUC Minas) and Jean-François Méhaut

9.2.3. Juries

9.2.3.1. Frédéric Desprez

- Nelson Lossing, reviewer, *Compilation pour machines à mémoire réparties: une approche multipasse*, PhD, Université de recherche Paris Science, April 3 2017
- Luis Pineda, reviewer, *Efficient Support for Data-Intensive Workflows on Geo-Distributed Clouds*, Université de Rennes, May 24 2017

- Adrien Lebre, member of the committee, *Contributions to Large-scale Distributed Systems The infrastructure Viewpoint*, Nantes, September 1 2017
- Thomas Gonçalves, Advisor with Jean-François Méhaut and Marc Pérache (CEA DAM), *Contributions à la parallélisation de méthodes de type transport Monte-Carlo*, PhD Université de Grenoble Alpes, September 28 2017
- Pierre Ramet, reviewer, *Heterogeneous architectures, Hybrid methods, Hierarchical matrices for Sparse Linear Solvers*, Université de Bordeaux, November 27 2017
- Pedro Silva, advisor with Christian Perez (Avalon), *On the mapping of distributed applications onto multiple Clouds*, ENS Lyon, December 11 2017
- Millian Poquet, chair, *Approche par la simulation pour la gestion de ressources*, Université de Grenoble Alpes, December 19 2017

9.2.3.2. Jean-François Méhaut

- Soraya Zertal, Reviewer, *Contributions to data storage systems: modelling, simulation and evaluation tools*, HDR Université de Versailles, November 2017
- Abdou Guermouche, Reviewer, *Towards Efficient Sparse Direct Solvers for Modern High-Performance Architectures*, HDR Université de Bordeaux, December 2017
- Vanessa Vargas, Advisor with Raoul Velzco (TIMA), *Approche logicielle pour améliorer la fiabilité d'applications parallèles implémentées sur des processeurs multi-cœurs et many-cœurs*, PhD Université de Grenoble Alpes, April 2017
- Thomas Gonçalves, Advisor with Marc Pérache (CEA DAM) and Frédéric Desprez, *Contributions à la parallélisation de méthodes de type transport Monte-Carlo*, PhD Université de Grenoble Alpes, September 2017
- Krishna Singh, Advisor with Stéphane Redon (LJK, Nano-D), *Algorithmes pour la dynamique moléculaire restreinte de manière adaptative*, PhD Université de Grenoble Alpes, November 2017

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

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Isabelle Puaut is Program Chair of the 2017 IEEE Real-Time Systems Symposium (RTSS), held in Paris, France. She is general Chair of RTSS 2018, to be held in Nashville, Tennessee.

9.1.2.2. Member of the Conference Program Committees

Sylvain Collange was PC member of Compas'2017.

Pierre Michaud was a member of the program committees of the ISCA 2017 and MICRO 2017 conferences.

Isabelle Puaut is member of the program committees of the Euromicro Conference on Real Time Systems (ECRTS) 2017 and 2018, the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2017 and 2018.

André Seznec is a member of IEEE Micro 2018 Top Picks selection committee.

André Seznec was a member of the IEEE Micro 2017 and SAMOS 2017 conference program committee.

9.1.2.3. Reviewer

Members of PACAP routinely review submissions to numerous international conferences and events.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

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

9.1.3.2. Reviewer - Reviewing Activities

Members of PACAP routinely review submissions to numerous international journals.

9.1.4. Invited Talks

Erven Rohou was invited to the seminar "WCET meets compilation". He presented an invited talk.

9.1.5. Leadership within the Scientific Community

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

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

9.1.6. Research Administration

Isabelle Puaut is member of the Research Council (Commission Recherche) of the University of Rennes I. She is member of the working group "Habilitation à Diriger des Recherches".

Isabelle Puaut is member of the board of directors (Conseil d'Administration) of ISTIC (computer science and electrical engineering departement of University of Rennes I).

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).

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

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Damien Hardy, Linux and C programming, 22 hours, L3, Université de Rennes I, France

Licence: Damien Hardy, Real-time systems, 46 hours, L3, Université de Rennes I, France

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

Master: Isabelle Puaut, Operating systems: concepts and system programming under Linux (SEL), 75 hours, M1, Université Rennes I, France

Master: Isabelle Puaut, Operating systems internals (NOY), 55 hours, M1, Université Rennes I, France

Master: Isabelle Puaut, Optimizing and Parallelizing Compilers (OPC), 6 hours, M2, Université Rennes I, France

Master: Isabelle Puaut, Real-time systems, 48 hours, M1, Université Rennes I, France

Master: Isabelle Puaut, Writing of scientific publications, 20 hours, M2/PhD, Université Rennes I, France

Master: Sylvain Collange, Parallel Programming, 22 hours, M1, Université Rennes I, France

Master: Sylvain Collange, GPU programming, 32 hours, M2, ESIR, France

Master: Sylvain Collange, Advanced computer architecture, 4 hours, M2, Université Rennes I, France

Master: Sylvain Collange, Advanced CUDA programming, 8 hours, M2, Université Pierre et Marie Curie Paris 6, France

Master: André Seznec, Advanced Architectures, 8 hours, M2, Université de Rennes I, France

9.2.2. Supervision

PhD: Nabil Hallou, *Runtime Optimization of Binary Through Vectorization Transformations*, Université Rennes I, Dec 2017, co-advisors E. Rohou and P. Clauss (EPI Camus Inria Strasbourg)

PhD: Andrea Mondelli, *Revisiting Wide Superscalar Microarchitecture*, Université Rennes I, Sep 2017, co-advisors P. Michaud and A. Seznec

PhD in progress: Rabab Bouziane, *Compilation techniques to exploit novel low-power architecture and technology solutions*, Université Rennes I, started Nov 2015, advisor E. Rohou and Abdoulaye Gamatié (LIRMM, Montpellier)

PhD in progress, Viet Anh Nguyen, *Worst-Case Execution Time (WCET) Estimation for Many-core Architectures*, Université Rennes I, started Jan 2015, co-advisors I. Puaut and D. Hardy.

PhD in progress, Benjamin Rouxel, *Code optimizations for WCET calculation on many-core platforms*, started Oct 2015, co-advisors I. Puaut (70 %) and S. Derrien (30 %) from the CAIRN group.

PhD in progress: Arif Ali Ana-Pparakkal, *Dynamic Function Specialization*, Université Rennes I, started Feb 2015, advisor E. Rohou

PhD in progress: Simon Rokicki, *Compilation dynamique hybride logiciel/matériel*, Université Rennes I, started Sep 2015, co-advisors E. Rohou and Steven Derrien (CAIRN)

PhD in progress: Kalitzidis Kleovoulos, *Ultrawide Issue Superscalar Processors*, Université Rennes I, started Dec 2016, advisor A. Seznec

PhD in progress: Niloofar Charmchi, *Hardware prefetching and related issues*, Université Rennes I, started Jan 2017, advisor A. Seznec

PhD in progress: Daniel Rodriguez Carvalho, *Towards a compressed memory hierarchy*, Université Rennes I, started Oct 2017, advisor A. Seznec

9.2.3. Juries

Isabelle Puaut was a member of the following committees:

- Antoine Blin, Vers une utilisation efficace des processeurs multi-cœurs dans les systèmes embarqués à criticités multiples, Université Pierre et Marie Curie (UPMC), January 2017 (reviewer)
- Laure Abdallah, Worst-case delay analysis of core-to-IO flows over many-cores architectures, Université de Toulouse, April 2017 (reviewer)
- Stefanos Skalistis, Efficient adaptive hard real-time multi-processor systems, École Polytechnique Fédérale de Lausanne (EPFL), October 2017 (reviewer)
- Fabrice Guet, Étude de l'application de la théorie des valeurs extrêmes pour l'estimation fiable et robuste du pire temps d'exécution probabiliste, Université de Toulouse, December 2017 (examiner)
- Nabil Hallou, Runtime optimization of binary through vectorization transformations, Université de Rennes I, December 2017 (examiner)
- Quentin Perret, Predictable execution on many-core processors, Université de Toulouse, April 2017 (examiner)
- Soukayna Msirdi, Modular Avionics Software Integration on Multi-Core COTS, Université de Toulouse, July 2017 (reviewer)

Erven Rohou was a member of the following committees:

- Nabil Hallou, Runtime optimization of binary through vectorization transformations, Université de Rennes I, December 2017.
- Laurent Georget, Suivi de flux d'information correct pour les systèmes d'exploitation Linux, Université de Rennes I, September 2017
- Mohammed Boussaa, Automatic Non-Functional Testing and Tuning of Configurable Generators, Université de Rennes I, September 2017.
- Thierno Barry, Sécurisation à la compilation de logiciels contre les attaques en fautes, Université de Lyon, CEA Grenoble, November 2017.
- Shixiong Xu, Data Layout Oriented Compilation Techniques in Vectorization for Multi-/Many-cores, Trinity College, Dublin, Ireland, June 2017.

Erven Rohou was an external expert in the recruitment committee of Alexandra Jimborean, Uppsala Universitet, Sweden.

Erven Rohou was a member of the selection committee of Université de Paris-Est Marne-la-Vallée.

9.3. Popularization

Nicolas Kiss, Damien Hardy and Erven Rohou presented a poster at the "European Cyber Week", organized by the "Pôle d'Excellence Cyber".

Erven Rohou presented a poster at the Teratec Café, describing the ANTAREX H2020 project.

AOSTE2 Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Steering Committees

- Liliana Cucu-Grosjen is member of the steering committees of the following conferences and workshops: RTSS, RTAS, RTNS, WMC, RTSOPS.
- Rob Davis is member of the steering committees of the following conferences and workshops: RTSS, RTAS, RTNS, WMC, RTSOPS.

10.1.1.2. Member of the Organizing Committees

- Liliana Cucu is Local Arrangement Chair of the 38th IEEE Real-time Systems Symposium (RTSS'17).

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Liliana Cucu: RTAS, RTNS, WFCS
- Robert Davis: RTSS, RTAS, RTNS
- Adriana Gogonel: ACM RACS, WMC
- Dumitru Potop-Butucaru: ACSD, EMSOFT
- Yves Sorel: DASIP

10.1.2.2. Reviewer

All members of the team are regularly serving as reviewers for the main scientific events of our domain: RTSS, RTAS, RTCSA, RTNS, DATE, ETFA, EMSOFT, DASIP, etc.

10.1.3. Journal

10.1.3.1. Reviewer - Reviewing Activities

All members of the team are regularly serving as reviewers for the main journals of our domain: Journal of Real-Time Systems, Journal of Systems Architecture, Leibniz Transactions on Embedded Systems, IEEE Transactions on Industrial Informatics, etc.

10.1.4. Invited Talks

- Liliana Cucu is keynote speaker at the 11th edition of CRTS, invited speaker at MMR'17 and MEFOSYLOMA seminar.

10.1.5. Leadership within the Scientific Community

Liliana Cucu and Rob Davis are the scientific organizers of the 2nd Dagstuhl seminar on mixed-criticality systems.

10.1.6. Scientific Expertise

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

10.1.7. Research Administration

- Liliana Cucu-Grosjean is member of Inria Evaluation Commission, co-chair of Inria Committes on gender equality and equal oportunities, and member of the CLHCST.
- Dumitru Potop-Butucaru is member of mobility grant commission for postdocs and invited professors.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

Master: Dumitru Potop Butucaru, A synchronous approach to the design of embedded real-time systems, 30h, M1, EPITA Engineering School, Paris France.

Master: Yves Sorel, Optimization of distributed real-time embedded systems, 38H, M2, University of Paris Sud, France.

Master: Yves Sorel, Synchronous languages and real-time scheduling, 9H, M2, University of Paris-Est Créteil, France.

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

10.2.2. Supervision

PhD: Cristian Maxim, End to end constraints using probabilistic approaches, UPMC, defended December 2017, supervised by Liliana Cucu.

PhD in progress: Slim Ben-Amor, Schedulability analysis of probabilistic real-time tasks under end to end constraints, UPMC, started on September 2016, supervised by Liliana Cucu.

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

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

PhD in progress: Evariste Ntaryamira, Analysis of embedded systems with time and security constraints, UPMC, started on January 2017, supervised by Liliana Cucu and Rachel Akimana.

PhD in progress: Walid Talaboulma, Probabilistic timing analysis in presence of dependences, UPMC, started 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 multiple control models, University of UMPC-Paris-Sorbonne, started December 2014, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel.

10.2.3. Juries

- Liliana Cucu is Phd reviewer for the thesis of Fabrice Guet, ONERA and ISAE, defended December 2017.
- Liliana Cucu is Phd reviewer for the thesis of Bader Alahmad, University of British Columbia, defended December 2017.
- Liliana Cucu is Phd jury member for the thesis of Romain Gratia, Telecom Paritech, defended January 2017.

10.3. Popularization

Popularization video of the probabilistic notions for mixed-criticality systems https://www.youtube.com/watch?v=sSJT4eGhS_A

HYCOMES Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Benoît Caillaud has organized the Synchron'17 open workshop on *Synchronous Programming Languages*[0] that took place at Inria Rennes from November 27th-30th 2017.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

Khalil Ghorbal served as a PC member in the Repeatability Evaluation Committee of HSCC (Hybrid Systems: Computation and Control) 2017.

Albert Benveniste served as a PC member of the International Modelica Conference 2017.

Benoît Caillaud has served on the Steering and Programme Committees of the ACSD'17 conference.

8.1.2.2. Reviewer

Khalil Ghorbal reviewed a paper for the IEEE Conference on Decision and Control 2017.

Albert Benveniste reviewed a paper for FoSSaCS (International Conference on Foundations of Software Science and Computation Structures) 2017.

Benoît Caillaud has reviewed one paper for the LICS'17 conference.

8.1.3. Journal

8.1.3.1. Reviewer - Reviewing Activities

Khalil Ghorbal reviewed a journal paper for the IEEE Transactions on Automatic Control.

Albert Benveniste reviewed a journal paper for the Science of Computer Programming journal.

Benoît Caillaud has reviewed papers for th IEEE Transactions on Control Systems Technology.

8.1.4. Invited Talks

Khalil Ghorbal was invited by Saman Zonouz. Rutgers University, NJ, USA.

Albert Benveniste gave an invited talk at the Laboratory for Information & Decision Systems, MIT, Cambridge, MA, USA.

8.1.5. Scientific Expertise

Albert Benveniste was a reviewer for the ERC Advanced Grant proposals 2017.

8.1.6. Research Administration

Benoît Caillaud is head of the *Language and Software Engineering Department* of IRISA (UMR 6074). The department is composed of 9 research teams and about 120 researchers and students, in Brest, Rennes and Vannes.

[0] https://synchron17.inria.fr

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, France.

Master : Khalil Ghorbal, *Analyse et Conception Formelles*, M1, (chargé de TD), 22h EqTD, University Rennes 1 and ENS Rennes, France

Master : Khalil Ghorbal, Solvers Principle and Architectures, M2, (enseignant principal), 30h EqTD, ENS Rennes, France

Master : Khalil Ghorbal, Modeling Physics with Differential-Algebraic Equations, M2, (enseignant principal), 25h EqTD, Ecole Polytechnique, Palaiseau, France

8.2.2. Supervision

PhD : Ayman Aljarbouh, *Accelerated Simulation of Hybrid Systems: Method combining static analysis and runtime execution analysis*, University of Rennes 1, defended 13/09/2017, supervised by Benoît Caillaud.

PhD : Guillaume Baudart, *A Synchronous Approach to Quasi-Periodic Systems*, Ecole Normale Superieure (Paris), defended 13/03/2017, co-supervised by Albert Benveniste.

8.2.3. Juries

Benoît Caillaud has been president of PhD defence jury of Mohamed Amine Aouadhi, on 29 September 2017, at LS2N, the University of Nantes, France.

Albert Benveniste participated in the jury of the PhD thesis of Guillaume Baudart.

KAIROS Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Eric Madelaine was General Chair of the 11th IEEE International conference on Theoretical Aspects of Software Engineering (TASE'2017), which was held in Sophia-Antipolis, september 2017. The whole conference was organized by the services of Inria Sophia Méditerranée Center.
- Marie-Agnès Peraldi-Frati and Frédéric Mallet organized the Workshop InS3Pect System engineering for Secured Services for Connected Objects. The workshop gathered approximately thirty researchers and industrials to explore a transdisciplinary approach for Connected Objects Secured Services modeling and validation https://www.i3s.unice.fr/ins3pect/fr/node/8/.

9.1.1.2. Member of the Organizing Committees

Frederic Mallet was a member of the organizing committee of COMPAS 2017, organized in Antibes from June 27th to 30th 2017 https://compas2017.sciencesconf.org/.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Robert de Simone: was Program Chair of EMSOFT 2017, part of the federated "superconference" ESWEEK 2017 (Seoul, Korea, October).
- Frédéric Mallet was Program Chair for TASE 2017.
- Eric Madelaine was Steering Committee Chair for the Int. Symposium on Formal Aspects of Component Software (FACS 2017).
- Frederic Mallet was steering committee member of ETR 2017

9.1.2.2. Member of Conference Program Committees

- Robert de Simone: FDL 2017, MEMOCODE 2017.
- Frederic Mallet: DATE 2017, Euromicro DSD 2017, FDL 2017, ModelsWard 2017, DHS 2017, ICTERI 2017.
- Julien Deantoni: Models 2017, DSD 2017, TASE 2017, Momo 2017, GEMOC 2017, EXE 2017, MDEbug 2017.
- Marie-Agnès Peraldi-Frati: national French Conférence en Ingénierie du Logiciel (CIEL).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Eric Madelaine was Guest Editor for the Science of Computer Programming journal, of a special issue on FACS 2016 selected papers.

9.1.4. Invited Talks

Sid Touati gave an Invited Tutorial entitled "Parametric statistics for program performance analysis, comparison and evaluation" at the 2017 International Conference on High Performance Computing and Simulation (HPCS 2017, Genova, Italy).
Eric Madelaine gave an invited seminar at ECNU Shanghai in Nov. 2017.

Frederic Mallet gave an invited talk on the "Model-Based System Engineering for Cyber-Physical Systems" at ECNU in Shanghai and in Suzhou University in December 2017. He also gave an invited talk together with Julien DeAntoni in the GT OVSTR of the Labex Digicosme in Telecom ParisTech in April 2017.
Julien Deantoni was invited speaker on the fourteenth Bellairs CAMPaM workshop on multi-paradigm modeling and simulation, in Barbados (http://msdl.cs.mcgill.ca/conferences/CAMPaM/2017/).

9.1.5. Leadership within the Scientific Community

Robert de Simone is Prime Investigator for the FM4CPS Associated-Team (with ECNU Shanghai); he is also Inria contact coordinator for the DESIR collaborative programme from SAFRAN on embedded system design.
Eric Madelaine is member of the Council Board of the International Joint Lab of Trustworthy Software (IJLTS), from ECNU Shanghai.

9.1.6. Research Administration

Robert de Simone was Deputy Director of the EDSTIC Doctoral School until September 2017.
Frederic Mallet is the deputy director of the I3S Laboratory (UMR 7271 CNRS UNS) and he is in charge of the relationships with LEAT and of the research formations. He is also a member of the Steering Committee of the Poˆle de Compétitivité Solutions Communicantes Sécurisées (SCS) and of its board. He is the head of the first Year of the International Track of the Master on Foundations of Computer Sciences.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

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

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

Master : Julien Deantoni, Finite State Machines, 24h, M1,Polytech'Nice, France.

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

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.

9.2.2. Supervision

- PhD: Emilien Kofman, *Conception Haut Niveau Low Power d'objets mobiles communicants*, 2017, supervised by Robert de Simone, co-supervised by François Verdier (UMR CNRS/UNS LEAT).
- PhD in progress: Hui (Vincent) Zhao, UNS, started February 2016, supervised by Frédéric Mallet, co-supervised by Ludovic Apvrille (Telecom ParisTech)
- PhD in progress: Dongdong An, ECNU-SEI/China, started November 2016, co-supervised by R. de Simone, supervised by Jing Liu (ECNU).

- PhD in progress: Pierre Leca, CIFRE thesis at Huawey Research Lab (Paris), started 2017, supervised by Gaetan Haines and Ludovic Henrio, co-advisor Eric Madelaine
- PhD in progress: Zhao Yanrui, ECNU-SEI/China, started in January 2017, co-supervised by Yixiang Chen (ECNU) and Frederic Mallet

9.2.3. Juries

Robert de Simone: Examiner (Président) for the PhD of Vincenzo Mastandrea (UCA)

Frédéric Mallet: Examiner (President) for the HDR of Jerome Hugues from ISAE Sup'Aero.

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 PLDI 2017.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Timothy Bourke was a member of the PC of EMSOFT 2017.
- Timothy Bourke was a member of the PC of the Modelica Conference 2017.
- Timothy Bourke was a member of the PC of SCOPES 2017.
- Timothy Bourke was a member of the Student Research Competition panel of PLDI 2017.
- Francesco Zappa Nardelli was a member of the PC of POPL 2017.
- Francesco Zappa Nardelli was a member of the PC of ECOOP 2017.
- Marc Pouzet was a member of the PC of SCOPES 2017, EOOLT 2017, FADL 2017.
- Albert Cohen was a PC member of CGO 2018, Supercomputing 2017, PACT 2017.
- Albert Cohen was the area co-chair for programming models at IPDPS 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Albert Cohen is associate editor of the ACM Transactions on Architecture and Code Optimization

9.1.3.2. Reviewer - Reviewing Activities

- Timothy Bourke was a reviewer for the Springer Real-Time Systems Journal.
- Timothy Bourke was a reviewer for IEEE Transactions on Software Engineering.

9.1.4. Invited Talks

- Timothy Bourke was invited to talk about the seL4 project at the Forum Méthodes Formelles: “Méthodes formelles et cyber-sécurité” in Toulouse in January 2017.
- Timothy Bourke was invited to speak on the “Verified Compilation of Lustre” at the University of Birmingham in March 2017.
- Francesco Zappa Nardelli is an invited speaker at the Entropy Workshop, January 2018.
- Francesco Zappa Nardelli was an invited speaker at Dagsthul Seminar 17502 “Testing and Verification of Compilers”, December 2017.
- Francesco Zappa Nardelli was an invited speaker at the ETH Workshop on Software Correctness and Reliability, October 2017.
- Marc Pouzet was an invited speaker of the GT OVSTR Digicosme (CEA - Telecom Paris), in April 2017; the GDR Glace (part of GPL), in June 2017.

9.1.5. Leadership within the Scientific Community

Albert Cohen is a steering committee member of the PLDI, PPoPP and Compiler Construction conferences.

9.1.6. Scientific Expertise

Albert Cohen has been a visiting scientist at Facebook Artificial Intelligence Research.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

Licence: F. Zappa Nardelli: “Concurrent Programming" (L3), PCs, 32h, E´cole Polytechnique, France

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

Master: M. Pouzet : “Synchronous reactive Languages” (M2), Lectures. Master Comasic (Polytechnique), France.

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

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

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

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

9.2.2. Supervision

- PhD : Guillaume Baudart, 3rd year, supervised by T. Bourke and M. Pouzet. This thesis was defended in March 2017.
- PhD in progress : Ulyssse Beaugnon, 3rd year, supervised by A. Cohen and M. Pouzet.
- PhD in progress : Lélio Brun, 2nd year, supervised by T. Bourke and M. Pouzet.
- PhD : Robin Morisset, 3rd year, supervised by F. Zappa Nardelli. This thesis was defended in April 2017.
- PhD in progress : Chandan Reddy, 3rd year, supervised by A. Cohen.
- PhD in progress : Jie Zhao, 3rd year, supervised by A. Cohen.

9.2.3. Juries

Francesco Zappa Nardelli was jury member of the PhD thesis of Yannick Zakowski, ENS Rennes, Dec 2017.

Francesco Zappa Nardelli will be jury member of the PhD thesis of Francois Ginraud, Grenoble, Jan 2018.

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 is member of the steering committee of the International Federated Conference on Distributed Computing Techniques (DISCOTEC) and of the ACM International Conference on Embedded Software (EMSOFT).
- Gregor Gössler is member of the steering committee of the International Workshop on Causal Reasoning for Embedded and Safety-critical Systems Technologies (CREST).

9.1.1.2. Member of the Organizing Committees

- Sophie Quinton was part of the organization committee of the 25th International Conference on Real-Time Networks and Systems (RTNS'17).
- Sophie Quinton was co-chair of the 2nd Tutorial on Tools for Real-Time Systems (TuToR'17), held as a satellite event of RTSS'17. http://tutor2017.inria.fr/
- Sophie Quinton was co-organizer of a tutorial entitled "Multicore Architectures in the Automotive Industry: Existing Solutions, Current Problems and Future Challenges" at ESWeek'17. http://2017.rtss.org/industrial-panel/
- Sophie Quinton was the organizer of a industry panel entitled "Beyond the Deadline: New Interfaces Between Control and Scheduling for the Design and Analysis of Critical Embedded Systems" at ESWeek'17. https://team.inria.fr/spades/beyond-the-deadline/

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Alain Girault was co-chair of the track "Model-based Design and Verification for Embedded Systems" of the Design Automation and Test in Europe Conference (DATE'17, track E3).
- Sophie Quinton was co-chair of the 8th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS'17), held as a satellite event of ECRTS'17. http://waters2017.inria.fr

9.1.2.2. Member of the Conference Program Committees

- Alain Girault served in the program committees of the Symposium on Industrial Embedded Systems (SIES'17) and the Forum on specification and Design Languages (FDL'17).
- Gregor Gössler served in the program committees of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE'17) and the 2nd international Workshop on Causal Reasoning for Embedded and Safety-critical Systems Technologies (CREST'17).
- Sophie Quinton served in the program committees of the 29th Euromicro Conference on Real-Time Systems (ECRTS'17) and the ACM SIGBED International Conference on Embedded Software (EMSOFT'17).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Alain Girault is a member of the editorial board of the Journal on Embedded Systems.

9.1.3.2. Reviewer – Reviewing Activities

- Alain Girault reviewed articles for IEEE Embedded Systems Letters (ESL), Microprocessors and Microsystems, IEEE Trans. on Industrial Informatics (TII), and ACM Trans. on Embedded Computing Systems (TECS).
- Gregor Gössler reviewed articles for Formal Methods in System Design (FMSD) and Engineering Applications of Artificial Intelligence (EAAI).

9.1.4. Research Administration

- Pascal Fradet is head of the committee for doctoral studies ("Responsable du comité des études doctorales") of the INRIA Grenoble – Rhône-Alpes research center and local correspondent for the young researchers INRIA mission ("Mission jeunes chercheurs").
- Alain Girault is vice-chair of the Inria Evaluation Committee.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

Licence : Pascal Fradet, Modèles de Calcul : λ-calcul, 12 HeqTD, niveau L3, Univ. Grenoble Alpes, France

Master : Pascal Fradet, Langages et Traducteurs, 16 HeqTD, niveau M1, Polytech Grenoble, Univ. Grenoble Alpes, France

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

Master : Xavier Nicollin, Sémantique et Analyse des Programmes, 45 HeqTD, niveau M1, Grenoble INP (Ensimag), France

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

Licence : Xavier Nicollin, Bases de la Programmation Impérative, 81 HeqTD (2016-2017), niveau L3, Grenoble INP (Ensimag), France

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

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

9.2.2. Supervision

- PhD in progress: Sihem Cherrared, "Fault Management in Multi-Tenant Programmable Networks", Univ. Rennes 1, since October 2016, co-advised by Eric Fabre and Gregor Gössler.
- PhD in progress: Christophe Prévot, "Early Performance assessment for evolving and variable Cyber-Physical Systems", Univ. Grenoble Alpes, since November 2015, co-advised by Alain Girault and Sophie Quinton.
- PhD in progress: Stephan Plassart, "On-line optimization in dynamic real-time systems", Univ. Grenoble Alpes, since September 2016, co-advised by Bruno Gaujal and Alain Girault.
- PhD in progress: Xiaojie Guo, "Formal Proofs for the Analysis of Real-Time Systems in COQ", Univ. Grenoble Alpes, since December 2016, co-advised by Pascal Fradet, Jean-François Monin, and Sophie Quinton.
- PhD in progress: Maxime Lesourd, "Generic Proofs for the Analysis of Real-Time Systems in COQ", Univ. Grenoble Alpes, since September 2017, co-advised by Pascal Fradet, Jean-François Monin, and Sophie Quinton.

- PhD in progress: Arash Shafiei, “Programming IoT and sofware defined radio with dynamic dataflow models of computation”, Univ. Grenoble Alpes, since September 2017, co-advised by Pascal Fradet, Alain Girault, and Xavier Nicollin.
- PhD in progress: Martin Vassor, “Analysis and types for safe dynamic software reconfigurations”, Univ. Grenoble Alpes, since November 2017, co-advised by Pascal Fradet and Jean-Bernard Stefani.
- M2 MOSIG: Leila Jamshidian Sales, “Towards a Dataflow Model of Computation (MoC) for Internet of Things (IoT)”, Univ. Grenoble Alpes and Grenoble INP, September 2017, co-supervised by Pascal Fradet, Alain Girault, and Xavier Nicollin.
- M2 MOSIG: Ebrahim Naeimimoshirian, “Hierarchical actor model with encapsulation”, Univ. Grenoble Alpes and Grenoble INP, September 2017, co-supervised by Xavier Nicollin and Jean-Bernard Stefani.

9.2.3. Juries

- Alain Girault was examiner for the PhD jury of Maalej Maroua (ENS-Lyon) and president for the PhD jury of Aurélien Cavelan (ENS-Lyon).
- Sophie Quinton was member of the PhD jury of Antoine Blin (U. Pierre et Marie Curie à Paris).

TEA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

Jean-Pierre Talpin served as General Chair and Finance Chair of the 15th. ACM-IEEE Conference on Methods and Models for System Design in Vienna.

10.1.1.2. 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. Member of the Conference Program Committees

Jean-Pierre Talpin served the program committee of:

- ACSD'17, 17th. International Conference on Application of Concurrency to System Design
- LCTES'17, 20th. ACM SIGPLAN-SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems
- SAC'18, 33rd. ACM SIGAPP Symposium on Applied Computing
- SCOPES'17, 20th. International Workshop on Software and Compilers for Embedded Systems

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).

10.1.3.2. Reviews

Thierry Gautier reviewed articles for *Information Processing Letters*.

10.1.4. Invited Talks

Jean-Pierre Talpin gave a keynote speech, entitled "Compositional methods for CPS design" at the Symposium on Dependable Software Engineering (SETTA'17) in Changsha, October 25.

10.1.5. Invited Talks

Albert Benveniste and Thierry Gautier previewed a seminar at SYNCHRON'17 to be given at the Collège de France in Gérard Berry's 2017-2018 lecture course.

10.1.6. Scientific Expertise

Jean-Pierre Talpin was nominated vice-president of ANR evaluation committee CES-25

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Jean-Pierre Talpin gave a one week class "Introduction to model-checking" at Nankai University in July and at Beihang University in November.

10.2.2. Supervision

Jean-Pierre Talpin co-supervises the PhD Thesis of Simon Lunel, Liangcong Zhang and Jean-Joseph Marty

10.2.3. Juries

Jean-Pierre Talpin served as rapporteur at the HDR Thesis defense of Jérôme Hugues, entitled “Architecture in the Service of Real-Time Middleware, Contributions to Architecture Description Languages”, which took place at INP Toulouse on February 22.

Jean-Pierre Talpin served as rapporteur at the HDR Thesis defense of Maxime Pelcat, entitled “Models, methods and tools for bridging the design productivity gap of embedded signal processing systems”, which took place at Institut Poincarré in Clermond-Ferrand on July 10.

ANTIQUE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Selection

10.1.1.1. Chair of Conference Program Committees

- Jerome Feret served as co-Chair of CMSB 2017 (Computational Methods in Systems Biology).
- Xavier Rival is serving as Chair of the Artifact Evaluation Committee of SAS 2018 (Static Analysis Symposium).

10.1.1.2. Member of the Conference Program Committees

- Jerome Feret served as a Member of the Program Committee of TMPA 2017 (Tools and Methods of Program Analysis).
- Jerome Feret served as a Member of the Program Committee of JOBIM 2017 (Journées Ouvertes en Biologie, Informatique et Mathématiques).
- Jerome Feret served as a Member of the Program Committee of SASB 2017 (Static Analysis and System Biology).
- Jerome Feret is serving as a Member of the Program Committee of LICS 2018 (Logic in Computer Science).
- Jerome Feret is serving as a Member of the Program Committee of VEMDP 2018 (Verification of Engineered Molecular Devices and Programs).
- Jerome Feret is serving as a Member of the Program Committee of SAS 2018 (Static Analysis Symposium).
- Jerome Feret is serving as a Member of the Program Committee of CMSB 2018 (Computational Methods in Systems Biology).
- Xavier Rival was a Member of the Program Committee of SAS 2017 (Static Analysis Symposium).
- Xavier Rival is serving as a Member of the Program Committee of SAS 2018 (Static Analysis Symposium).
- Xavier Rival was a Member of the Program Committee of Web Design, Analysis, Programming and Implementation of the WWW'18 Conference.
- Xavier Rival was a Member of the Extended Review Committee of PLDI 2018 (Programming Languages Design and Implementation).
- Cezara Dragoi was a member of Programming languages design and implementation PLDI'17.
- Cezara Dragoi was a member of Computer Aided Verification CAV'18.

10.1.1.3. Reviewer

- Jerome Feret served as reviewer for CONCUR 2017 (Concurrency Theory).
- Jerome Feret served as reviewer for LICS 2017 (Logic in Computer Science).
- Jerome Feret served as reviewer for VMCAI 2017 (Verification, Model Checking, and Abstract Interpretation).

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

- Jerome Feret is a member of the editorial board of the Frontiers in Genetics journal and the Open Journal of Modeling and Simulation.
- Jerome Feret serves as co-Editor of an Issue of the Theoretical Computer Science journal, that is composed of papers from SASB 2016, and is expected to appear in 2018.
- Jerome Feret serves as Editor of an Issue of the IEEE/ACM Transactions on Computational Biology and Bioinformatics, that is composed of papers from CMSB 2016, and is expected to appear in 2019.
- Xavier Rival serves as Editor of an Issue of the Formal Methods in System Design Journal, that is composed of a selection of papers from SAS 2016, and is expected to appear in 2018.

10.1.2.2. Reviewer - Reviewing Activities

- Jerome Feret served as a Reviewer for FMSD (Formal Methods in System Design).
- Jerome Feret served as a Reviewer for TCS (Theoretical Computer Sciences).
- Jerome Feret served as a Reviewer for TCBB (IEEE/ACM Transactions on Computational Biology and Bioinformatics).
- Jerome Feret served as a Reviewer for TCL (Transactions on Computational Logic).
- Xavier Rival served as a Reviewer for ACM TOPLAS (Transactions On Programming Languages and Systems).
- Xavier Rival served as a Reviewer for ACM TOPS (Transactions On Privacy and Security).

10.1.3. Invited Talks

- Jerome Feret gave a talk on automatic reduction of models of intra-cellular signaling pathways at the Dagstuhl Seminar on Algorithmic Cheminformatics (5–10 November 2017).
- Cezara Dragoi was invited speaker at the 6th South of England Regional Programming Language Seminar University College London, Workshop on Software Correctness and Reliability at ETH Zurich, and Workshop on Formal Reasoning in Distributed Algorithms (FRIDA), Wien Austria.

10.1.4. Leadership within the Scientific Community

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

10.1.5. Research Administration

Jerome Feret and Xavier Rival are members of the Laboratory Council of DIENS.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence:

- Jerome Feret, and Marc Chevalier, Mathematics, 40h, L1, FDV Bachelor program (Frontiers in Life Sciences (FdV)), Université Paris-Descartes, France.
- Jerome Feret and Xavier Rival, “Semantics and Application to Verification”, 36h, L3, at École Normale Supérieure, France.
- Xavier Rival, “Introduction to Static Analysis”, 8h, L3, at École des Mines de Paris, France.
- Xavier Rival “Programmation Avancée”, 18h, L3, at École Polytechnique, France.
- Cezara Dragoi “Les principes des langages de programmation”, 18h, L1, at École Polytechnique, France.

Master:

- Xavier Rival, “Verification” Lab Course, 20h, M1, École Polytechnique, France.

- Xavier Rival, “Protocol Safety and Verification”, 12h, M2, Advanced Communication Networks Master, France.
- Xavier Rival, “Program Analysis”, 24h, M2, Korea Advanced Institute for Science and Technology (KAIST), South Korea.
- Cezara Drăgoi, Jerome Feret, Antoine Miné, and Xavier Rival, “Abstract Interpretation: application to verification and static analysis”, 72h, M2. Parisian Master of Research in Computer Science (MPRI), France.
- Vincent Danos and Jerome Feret (with Jean Krivine), Computational Biology, 28h, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.

10.2.2. Supervision

- PhD defended: Ferdinanda Camporesi, Formal and exact reduction for differential models of signaling pathways in rule-based languages. Defended the 23th of January, 2017 and supervised by Jerome Feret.
- PhD in progress: Marc Chevalier, Static analysis of Security Properties in Critical Embedded Software. started in 2017 and supervised by Jerome Feret
- PhD in progress: Hugo Illous, Relational Shape Abstraction Based on Separation Logic, started in 2015 and supervised by Xavier Rival and Matthieu Lemerre (CEA)
- PhD in progress: Huisong Li, Disjunctive Shape Abstraction for Shared Data-Structures, started in 2014 and supervised by Xavier Rival
- PhD in progress: Jiangchao Liu, Static Analysis for Numeric and Structural Properties of Array Contents, started in 2014 and supervised by Xavier Rival

10.2.3. Juries

- Jerome Feret served as a member of the Jury of the PhD of Jean Coquet (Defended the 20th of December, 2017).
- Xavier Rival served as a Reviewer in the Jury of the PhD of Ahmad Salim Al-Sibahi (Defense planned for the 11th of January, 2018).

10.2.4. Responabilities

- Jerome Feret is a member of the Monotoring Committee for PhD Studies (CSD) of Inria Paris.
- Jerome Feret is deputy head of studies of the Computer Science department of École normale supérieure.

10.2.5. Selection committees

- Jerome Feret was a member of the recruitment committee for an assistant professor in Evry University 2017.
- Jerome Feret is a member of the recruitment committee for an assistant professor in Paris-Diderot University 2018.

CELTIQUE Project-Team

6. Dissemination

6.1. Promoting Scientific Activities

6.1.1. Scientific Events Selection

6.1.1.1. Chair of Conference Program Committees

- CoqPL 2017 (International Workshop on Coq for PL) was chaired by Sandrine Blazy and Emilio Jesus Gallego Arias

6.1.1.2. Member of the Conference Program Committees

- TASE 2017 (Symposium on Theoretical Aspects of Software Engineering): Alan Schmitt
- Web Programming 2018: Alan Schmitt
- ProWeb 2018: Alan Schmitt
- CC 2017 (Conference on Compiler Construction) : David Pichardie
- ESORICS 2017 (European Symposium on Research in Computer Security) : David Pichardie
- ESOP 2017 (European Symposium on Programming) : David Pichardie
- CC 2018 (Conference on Compiler Construction) : David Pichardie
- CoqPL 2017 (International Workshop on Coq for PL) : Sandrine Blazy
- AFADL 2017 (Approches Formelles dans l'Assistance au Développement de Logiciels) : Sandrine Blazy
- SRC (Student Research Competition) @ PLDI 2017 : Sandrine Blazy
- VSTTE 2017 (Verified Software: Theories, Tools, and Experiments) : Sandrine Blazy
- GPCE 2017 (Generative Programming: Concepts & Experiences) : Sandrine Blazy
- IFL 2017 (International symposium on Implementation and application of Functional Languages) : Sandrine Blazy
- TFP 2017 (Trends in Functional Programming) : Sandrine Blazy
- CPP 2018 (ACM SIGPLAN Conference on Certified Programs and Proofs) : Sandrine Blazy
- Euro S&P 2018 (IEEE European Symposium on Security and Privacy) : Sandrine Blazy
- TACAS 2017 (Tools and Algorithms for the Construction and Analysis of Software : Thomas Jensen.
- FCS 2017 (Int. workshop on Foundations of Computer Security) : Thomas Jensen.
- SAS 2017 (Static Analysis Symposium) : Thomas Jensen.

6.1.1.3. Reviewer

- POPL 2018 (Symposium on Principles of Programming Languages): Alan Schmitt

6.1.2. Journal

6.1.2.1. Reviewer - Reviewing Activities

- Information & Computation: Alan Schmitt
- Science of Computer Programming: Alan Schmitt
- Discrete Mathematics & Theoretical Computer: Alan Schmitt
- Theoretical Computer Science: Alan Schmitt
- Journal of Logical and Algebraic Methods in Programming: Alan Schmitt

- ACM Transactions on Privacy and Security (TOPS): David Pichardie

6.1.3. Invited Talks

- Delphine Demange: "On-the-Fly Garbage Collection: An Exercise in Compiler Verification". Inria Scientific Days 2017. June 2017.
- Thomas Genet: "SPAN+AVISPA for Verifying Cryptographic Protocols". RESSI (Rendez-vous de la recherche et de l'enseignement de la sécurité des systèmes d'information), Grenoble, May 2017 [42].
- Thomas Genet: "Tree Automata for Reachability in Rewriting". International School on Rewriting, Eindhoven, July 2017. http://www.win.tue.nl/~hzantema/isr.html.
- Thomas Jensen: Formal methods for software security, Forum Méthodes Formelles, Toulouse, France, Jan. 2017 [21].
- Thomas Jensen: Formal methods for software security, Journée inaugurale GDR Sécurité Informatique, Paris, June 2017 [22].
- Thomas Jensen. Hybrid information flow analysis against web tracking.. The 12th International Conference on Risks and Security of Internet and Systems (CRiSIS 2017), Dinard, France, Sept. 2017 [23].

6.1.4. Scientific Expertise

- Sandrine Blazy: expertise of an ERC Advanced Grant research proposal.
- Thomas Jensen is Inria representative in the European Cyber Security Organisation (ECSO) working group in Research and Innovation.

6.1.5. Research Administration

- Sandrine Blazy is member of Section 6 of the national committee for scientific research CoNRS.
- Sandrine Blazy is coordinator of the LTP (Languages, Types, Proofs) group of the French GDR GPL.
- Thomas Jensen is head of the NUMERIC department at Université Bretagne Loire.
- Thomas Jensen is director of the IT Security track and member of the executive board of the Laboratoire d'excellence "CominLabs".

6.2. Teaching - Supervision - Juries

6.2.1. Teaching

Licence : Alan Schmitt, Programmation Fonctionnelle, 36h, L3, Insa Rennes, France

Licence : Delphine Demange, Spécialité Informatique 1 - Algorithmique et Complexité Expérimentale, 36h, L1, Université Rennes 1, France

Licence : Delphine Demange, Spécialité Informatique 2 - Functional and Immutable Programming, 70h, L1, Université Rennes 1, France

Licence : Delphine Demange, Programmation de Confiance, 36h, L3, Université Rennes 1, France

Licence : David Pichardie, Graph algorithms, 24h, L3, ESIR, France

Licence : Sandrine Blazy, Functional programming, 30h, L3, Université Rennes 1, France

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

Licence : Thomas Genet, Spécialité Informatique 1 - Algorithmic and Experimental Complexity, 42h, L1, Université Rennes 1, France

Master : Sandrine Blazy, Méthodes Formelles pour le développement de logiciels sûrs, 53h, M1, Université Rennes 1, France

Master : Alan Schmitt, Méthodes Formelles pour le développement de logiciels sûrs, 25h, M1, Université Rennes 1, France France

Master : Sandrine Blazy, Mechanized Semantics, 15h, M2, Université Rennes 1, France

Master : Sandrine Blazy, Semantics, 24h, M1, Université Rennes 1, France

Master : Sandrine Blazy, Software vulnerabilities, 20h, M2, Université Rennes 1, France

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

Master : David Cachera, Semantics, 24h, M1, Université Rennes 1, France

Master : David Cachera, Advanced Semantics, 20h, M2, Université Rennes 1, France

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

Master : Thomas Jensen, Program Analysis and Software Security, 21h, M2, Université Rennes 1, France

6.2.2. Supervision

PhD in progress : Timothée Haudebourg, Lightweight Formal Verification for Functional Programs, 1st october 2017, Thomas Genet and Thomas Jensen

PhD in progress : Alexandre Dang, Security by compilation, 1st september 2016, Frédéric Besson and Thomas Jensen

PhD in progress : Julien Lepiller, Binary analysis for Isolation, 1st september 2016, Frédéric Besson and Thomas Jensen

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

PhD in progress : Florent Saudel, Vulnerability discovery, November 2015, Sandrine Blazy, Frédéric Besson and Cédric Berthion (Amossys)

PhD in progress : Alix Trieu, Formally verified compilation and static analysis, January 2016, Sandrine Blazy and David Pichardie

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

David Bühler, Structuring an abstract interpreter through value and state abstractions, defended March 2017, Sandrine Blazy and Boris Yakobowski (CEA)

Yannick Zakowski, Verification of a Concurrent Garbage Collector, defended December 2017, David Pichardie and David Cachera.

Pauline Bolignano, Formal models and verification of memory management in a hypervisor, defended May 2017, Thomas Jensen and Vincent Siles (Prove & Run).

Oana Andreescu, Static analysis of functional programs with an application to the frame problem in deductive verification, May 2017, Thomas Jensen and Stéphane Lescuyer (Prove & Run).

6.2.3. Juries

- Alan Schmitt, jury member for the selection of Inria CR (researcher) candidates, March and April 2017, Inria, Rennes, France.
- Thomas Jensen, jury member for the selection of Inria CR (researcher) candidates, March and April 2017, Inria, Rennes, France.
- Sandrine Blazy, jury member for the selection of CNRS CR and DR (researchers) candidates, February and March 2017, CNRS, Paris, France.
- Sandrine Blazy, jury member for the selection of a professor at University of Copenhagen, May 2017, Copenhagen, Denmark.
- Sandrine Blazy, jury member (reviewer) for the PhD defense of Romain Aïssat, January 2017, Paris-Sud University

- Sandrine Blazy, jury member for the PhD defense of Oana Andreescu, May 2017, Université Rennes 1
- Sandrine Blazy, jury member for the PhD defense of Ninon Eyrolles, June 2017, Université Versailles Saint-Quentin
- Sandrine Blazy, jury member (reviewer) for the HDR defense of Alain Giorgetti, December 2017, Université de Franche-Comté
- Sandrine Blazy, jury member for the PhD defense of Jordy Ruiz, December 2017, Université de Toulouse
- Sandrine Blazy, jury member for the PhD defense of Pierre Lestringant, December 2017, Université Rennes 1.
- Sandrine Blazy, jury member of the GDR GPL PhD award committee.
- David Pichardie, external reviewer for the PhD defense of Hendra Gunadi, July 2017, Australian National University, Canberra, Australia.
- David Pichardie, Licenciate discussion leader for the PhD student Marco Vassena, Chalmers University of Technology, Gothenburg, Sweden.
- Delphine Demange, jury member of the Gilles Kahn PhD award committee, December 2017, Inria Paris
- Delphine Demange, jury member for the PhD defense of Pauline Bolignano, May 2017, Université Rennes 1
- Thomas Genet, jury member (reviewer) for the PhD defense of Vivien Pelletier, October 2017, Université d'Orléans, France.
- Thomas Jensen, jury member for the HdR defense of Charlotte Truchet, November 2017, Université de Nantes, France.
- Thomas Jensen, jury member (reviewer) for the PhD defense of Zeineb Zhioua, September 2017, Téleécom ParisTech, France.
- Thomas Jensen, jury member for the PhD defense of Deepak Subramanian, December 2017, CentraleSupélec, France.

6.3. Popularization

Article "JavaScript, un langage à la croissance organique", Alan Schmitt, blog Binaire Le Monde. http://binaire.blog.lemonde.fr/2017/05/12/javascript-un-langage-a-la-croissance-organique/

Article "L'assistant de preuve Coq", Sandrine Blazy, Pierre Castéran, Hugo Herbelin, Techniques et Sciences de l'ingénieur, août 2017. https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/programmation-42304210/coq-assistant-de-preuve-h3310/

Talk "Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.", Thomas Genet, given three times in high schools close to Rennes.

CONVECS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

- H. Garavel is a member of the model board [0] of MCC (*Model Checking Contest*). In 2017, he helped preparing new models (especially those in the NUPN format) and verified, using the CÆSAR.BDD tool of CADP, the forms describing all benchmark models submitted by the contest participants; this revealed a number of inconsistencies. The results of MCC'2017 have been published online [45] and a journal paper is in preparation.
- Together with Peter Höfner (Data61, CSIRO, Sydney, Australia), H. Garavel set up a model repository (hosted on the Gforge of Inria) to collect and archive formal models of real systems; this infrastructure is used by the series of MARS workshops [0]. This repository currently contains 17 models, two of which (a Message Authenticator Algorithm and a Production Cell) were deposited in 2017 by CONVECS.
- G. Salaün is member of the steering committee of the SEFM (*International Conference on Software Engineering and Formal Methods*) conference series since 2014.
- G. Salaün is member of the steering committee of the FOCLASA (*International Workshop on Foundations of Coordination Languages and Self-Adaptative Systems*) workshop series since 2011.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- G. Barbon was publicity chair of FOCLASA'2017 (*15th International Workshop on Foundations of Coordination Languages and Self-Adaptative Systems*) co-located with SEFM'2017 (*15th International Conference on Software Engineering and Formal Methods*), Trento, Italy, September 5, 2017.
- F. Lang was co-chair of the Formal Methods track of ETR'2017 (*9ème Ecole d'été Temps-Réel*), Paris, France, August 28 - September 1, 2017.
- R. Mateescu was tutorial chair of QRS'2017 (*IEEE International Conference on Software Quality, Reliability, and Security*), Prague, Czech Republic, July 25–29, 2017.
- G. Salaün was co-chair of FOCLASA'2017.

9.1.2.2. Member of the Conference Program Committees

- H. Garavel was program committee member of the 7th FMF (*Forum Methodes Formelles*), Toulouse-Grenoble-Saclay-Rennes, France, January 31, 2017.
- H. Garavel was program committee member of MARS'2017 (*2nd Workshop on Models for Formal Analysis of Real Systems*), Uppsala, Sweden, April 29, 2017.
- H. Garavel and G. Salaün were program committee members of SEFM'2017 (*15th International Conference on Software Engineering and Formal Methods*), Trento, Italy, September 6–10, 2017.
- H. Garavel was program committee member of the 8th FMF (*Forum Methodes Formelles*), Toulouse-Grenoble-Saclay-Rennes, France, October 10, 2017.

[0] http://mcc.lip6.fr/models.php

[0] http://www.mars-workshop.org/

- F. Lang was program committee member of GaM'2017 (*3rd Workshop on Graphs as Models*), Uppsala, Sweden, April 22–23, 2017.
- R. Mateescu was program committee member of FMICS-AVoCS'2017 (*International Workshop on Formal Methods for Industrial Critical Systems and Automated Verification of Critical Systems*), Torino, Italy, September 18–20, 2017.
- G. Salaün was program committee member of PDP-4PAD'2017 (*25th Euromicro International Conference on Parallel, Distributed and Network-based Processing - Formal Approaches to Parallel and Distributed Systems*), St. Petersburg, Russia, March 6–8, 2017.
- G. Salaün was program committee member of SAC-SOAP'2017 (the *Service-Oriented Architectures and Programming* track) of SAC'2017 (*32nd ACM Symposium on Applied Computing*), Marrakesh, Morocco, April 3–7, 2017.
- G. Salaün was program committee member of SAC-SVT'2017 (the *Software Verification and Testing* track) of SAC'2017, Marrakesh, Morocco, April 3–7, 2017.
- G. Salaün and W. Serwe were program committee members of FSEN'2017 (*7th IPM International Conference on Fundamentals of Software Engineering*), Tehran, Iran, April 26–28, 2017.
- G. Salaün was program committee member of the poster track of ICSE'2017 (*39th International Conference on Software Engineering*), Buenos Aires, Argentina, May 20–28, 2017.
- G. Salaün was program committee member of COORDINATION'2017 (*19th International Conference on Coordination Models and Languages*), Neuchâtel, Switzerland, June 19–22, 2017.
- G. Salaün was program committee member of COMPSAC'2017 (*IEEE International Conference on Computers, Software, and Applications*), Torino, Italy, July 4–8, 2017.
- G. Salaün was program committee member of VBSP'2017 (*1st International Workshop on Verification of Business and Software Processes*), Paris, France, July 5, 2017.
- G. Salaün was program committee member of FACS'2017 (*14th International Conference on Formal Aspects of Component Software*), Braga, Portugal, October 10–13, 2017.
- G. Salaün was program committee member of Microservices'2017, Odense, Denmark, October 25–26, 2017.

9.1.2.3. Reviewer

- G. Barbon was a reviewer for COMPSAC'2017, SEFM'2017, and SAC-SVT'2018 (*33nd ACM Symposium on Applied Computing - Software Verification and Testing Track*), Pau, France, April 9–13, 2018.
- F. Lang was a reviewer for SEFM'2017 and FMICS-AVoCS'2017.
- L. Marsso was a reviewer for MARS'2017, COMPSAC'2017, SEFM'2017, and FMICS-AVoCS'2017.
- U. Ozeer was a reviewer for SEFM'2017.
- G. Salaün was a reviewer for MARS'2017.
- W. Serwe was a reviewer for MARS'2017, SEFM'2017, and ICTSS'2017 (*19th International Conference on Testing Software and Systems*), Paris, France, August 28–29, 2017.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

9.1.3.2. Reviewer - Reviewing Activities

- F. Lang was a reviewer for STTT.
- R. Mateescu was a reviewer for STTT.

- W. Serwe was a reviewer for STTT, SPE (*Journal on Software: Practice and Experience*), and IJPEDS (*International Journal on Power Electronics and Drive Systems*).
- G. Salaün was a reviewer for JSC (*Journal of Symbolic Computation*), IEEE TSE (*Transactions of Software Engineering*), and SCP (*Science of Computer Programming*).

9.1.4. Software Dissemination and Internet Visibility

The CONVECS project-team distributes several software tools, among which the CADP toolbox.

In 2017, the main facts are the following:

- We prepared and distributed twelve successive versions (2017-a to 2017-l) of CADP.
- We were requested to grant CADP licenses for 315 different computers in the world.

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

H. Garavel started a major rewrite of CorTeX, a build system and a collection of tools for documents prepared using LaTeX.

By the end of December 2017, the CADP forum [0], opened in 2007 for discussions regarding the CADP toolbox, had over 414 registered users and over 1796 messages had been exchanged.

Also, for the 2017 edition of the Model Checking Contest, three families of models generated using CADP (totalling 64 Nested-Unit Petri Nets) were provided.

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 COSTO tool for analyzing Kmelia components and services [48], [21]
- The VERCORS Platform for Model Checking Distributed Components [20]
- A Model-Driven and Multi-Agent Approach for Web Services Composition [19]
- Formal Analysis of Security Guidelines for Program Certification [57], [56], [58]
- A Product-Line for Families of Program Translators [22]
- The GROOVE Tool for Verification Based on Graph Rewriting [44]
- The FTRES Tool for Rare Event Simulation in Dynamic Fault Trees [52]
- The MIstRAL Tool for Middleware Reconfiguration Based on Formal Methods [51]
- The ALVIS Modelling Language for Embedded Systems [54]
- Adaptive Service Composition based on Runtime Verification of Formal Properties [23]

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

- Assisting Refinement and Formal Verification in the Design of Embedded Systems [49]
- A Formal Model for Plastic Human Computer Interfaces [25]
- Verifying Concurrent Stacks by Divergence-Sensitive Bisimulation [55]
- Compositional Model Checking of Liveness Properties [59]
- Verification of Visibility-Based Properties on Multiple Moving Robots [53]

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

9.1.5. Invited Talks

- G. Barbon gave a talk entitled “*Debugging of Concurrent Systems using Counterexample Analysis*” on March 2nd, 2017 at the 2nd year PhD student day of the LIG.
- G. Barbon gave a talk entitled “*Debugging of Concurrent Systems using Counterexample Analysis*” on December 13, 2017 at the *Journée scientifique du pôle MSTIC*.
- H. Garavel gave two talks entitled “*Ten Different Ways on Defining Signed Integers Formally*” and “*Benchmarking Implementations of Conditional Term Rewrite Systems*” on February 28, 2017 at the Formal Methods seminar of Inria Grenoble – Rhône-Alpes.
- H. Garavel gave a talk entitled “*Nested-Units Petri Nets*” during OPCT’2017 (*Open Problems in Concurrency Theory*), a research seminar co-sponsored by the IFIP Working Group 1.8, that took place in the Institute of Science and Technology Austria (IST Austria), Vienna, on June 26–29, 2017.
- H. Garavel gave a talk entitled “*From LOTOS to LNT*” during the ModelEd, TestEd, TrustEd Symposium in honour of the 60th birthday of Ed Brinksma held at the University of Twente, The Netherlands, on October 18, 2017.
- The members of CONVECS attended the 1st RIDINGS Workshop, held at Inria Grenoble – Rhône-Alpes on May 17, 2017. F. Lang gave a talk entitled “*The LNT language and the LNT2LOTOS compiler*”. H. Garavel gave a talk entitled “*The Unheralded Value of the Multiway Rendezvous: Illustration with the Production Cell Benchmark*”. L. Marsso gave a talk entitled “*A Large Term Rewrite System Modelling a Pioneering Cryptographic Algorithm*”. G. Barbon gave a talk entitled “*Debugging of Concurrent Systems using Counterexample Analysis*”.
- L. Marsso gave a talk entitled “*Formal Methods for Testing Networks of Controllers*” on May 29, 2017 at the 1st year PhD student day of the LIG.
- L. Marsso gave a talk entitled “*Formal Methods for Testing Networks of Controllers*” at the Scientific day of the ARC6 held at Université Grenoble Alpes, on November 23, 2017.
- L. Marsso and W. Serwe attended the 2nd RIDINGS Workshop held at Technical University Graz, Austria, on November 15, 2017. L. Marsso gave a talk entitled “*Testor: A Modular Tool for On-the-Fly Conformance Test Case Generation*”. W. Serwe gave a talk entitled “*Using a Formal Model to Improve Verification of a Cache-Coherent System on Chip*”.
- U. Ozeer gave a talk entitled “*Autonomous Resilience of Applications in a Largely Distributed Cloud Environment*” on May 29, 2017 at the 1st year PhD student day of the LIG.
- U. Ozeer gave a talk entitled “*Autonomous Resilience of Distributed IoT Applications in a Fog Environment*” at the IO Labs seminar held at Inria Paris on October 19–20, 2017.
- G. Salaün gave a talk entitled “*Checking Business Process Evolution*” on June 6, 2017 at the University of Málaga, Spain.

9.1.6. Research Administration

- H. Garavel was appointed to the Executive Commission in charge of International Relations at COMUE Université Grenoble Alpes.
- F. Lang is chair of the “*Commission du développement technologique*”, which is in charge of selecting R&D projects for Inria Grenoble – Rhône-Alpes.
- R. Mateescu is the scientific correspondent of the European and International Partnerships 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 Committee of the PCS action of the PERSYVAL Labex.

- W. Serwe is (together with Laurent Lefèvre from the AVALON Inria project-team) correspondent in charge of the 2017 Inria activity reports at Inria Grenoble – Rhône-Alpes.
- W. Serwe is a member of the "*Comité de Centre*" at Inria Grenoble – Rhone-Alpes.
- W. Serwe is "*chargé de mission*" for the scientific axis *Formal Methods, Models, and Languages* of the LIG laboratory.

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 Université Grenoble Alpes (UGA).

In 2017, we carried out the following teaching activities:

G. Barbon gave a tutorial course on "*Language Theory*" (18 hours "*équivalent TD*" on formal languages, automata, regular expressions, and grammars) to second year students of ENSIMAG.

H. Garavel, together with Laurence Pierre (TIMA, Grenoble), created a new curriculum HECS [0] ("*High-confidence Embedded and Cyberphysical Systems*") for 2nd-year MOSIG (*Master of Science in Informatics at Grenoble*) students. This curriculum opened for the first time in September 2016.

F. Lang, R. Mateescu, G. Salaün, and W. Serwe gave lectures on models for concurrency, temporal logics, equivalences, formal languages and verification (36 hours "*équivalent TD*") as part of the MOSIG/MACS-2 course ("*Modeling and Analysis of Concurrent Systems*") led by G. Salaün.

G. Barbon and W. Serwe supervised each a group of six teams in the context of the "*projet Génie Logiciel*" (55 hours "*équivalent TD*", consisting in 16 hours of lectures, plus supervision and evaluation), ENSIMAG, January 2017.

F. Lang gave a lecture on "*Modélisation et Vérification des Systèmes Concurrents et Temps-Réel*" (27 hours "*équivalent TD*") to third year students of ENSIMAG.

F. Lang gave a course on "*Formal Software Development Methods*" (7.5 hours "*équivalent TD*") in the framework of the "*Software Engineering*" lecture given to first year students of the MOSIG.

L. Marsso gave a course on "*Algorithms and Web Programming*" (44 hours "*équivalent TD*") at the department MMI of IUT1 (UGA).

G. Salaün taught about 200 hours of classes (algorithmics, Web development, object-oriented programming, iOS programming) at the department MMI of IUT1 (UGA). He is also headmaster of the "*Services Mobiles et Interface Nomade*" (SMIN) professional licence (3rd year of university) at IUT1/UGA.

9.2.2. Supervision

PhD in progress: G. Barbon, "*Debugging Concurrent Programs using Model Checking and Mining Techniques*", Université Grenoble Alpes, since October 2015, G. Salaün and V. Leroy

PhD in progress: L. Marsso, "*Formal Methods for Testing Networks of Controllers*", Université Grenoble Alpes, since October 2016, R. Mateescu, W. Serwe, I. Parissis, and Ch. Deleuze

PhD in progress: A. Muroor Nadumane, "*Softwarization of Everything: IoT Service Composition*", Université Grenoble Alpes, since October 2017, G. Salaün, R. Mateescu, L. Noirie, and M. Le Pallec

PhD in progress: U. Ozeer, "*Autonomous Resilience of Applications in a Largely Distributed Cloud Environment*", Université Grenoble Alpes, since November 2016, X. Etchevers, G. Salaün, F.-G. Ottogalli, and J.-M. Vincent

9.2.3. Juries

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

- R. Mateescu was reviewer of Alexandre Duret-Lutz's Habilitation thesis, entitled "*Contributions to LTL and Omega-Automata for Model Checking*", defended at EPITA (Paris, France) on February 10, 2017.
- R. Mateescu was reviewer of Zhengkui Zhang's PhD thesis, entitled "*Time and Cost Optimization of Cyber-Physical Systems by Distributed Reachability Analysis*", defended at the University of Aalborg (Denmark) on March 28, 2017.
- R. Mateescu was reviewer of Simon Busard's PhD thesis, entitled "*Symbolic Model Checking of Multi-Modal Logics: Uniform Strategies and Rich Explanations*", defended at Université Catholique de Louvain (Belgium) on May 10, 2017.
- G. Salaün was reviewer of Imen Boudhiba's PhD thesis, entitled "*A Model-Based Testing framework for IOSTS enriched with function calls*", defended at Centrale-Supélec (Paris, France) on March 2, 2017.
- G. Salaün was PhD committee president of Hosein Nazarpour's PhD thesis, entitled "*Monitoring Multi-threaded and Distributed (Component-Based) Systems*", defended at Université Grenoble Alpes on June 26, 2017.
- G. Salaün was PhD committee president of Jean-François Weber's PhD thesis, entitled "*Guiding and Controlling the Reconfigurations of Component-based Systems*", defended at Université de Franche-Comté (Besançon, France) on October 5, 2017.

9.3. Popularization

H. Garavel participates to the program committee and organization committee of FMF (*Formal Methods Forum*) [0], a series of industrial conferences on formal methods set up by the competitivity clusters Aerospace Valley and Minalogic, with the support of Inria and many other partners. The 7th FMF conference, devoted to formal methods and cybersecurity, was held on January 31, 2017. The 8th FMF conference, devoted to formal methods and autonomous vehicles, was held on October 10, 2017. Both events gathered a large audience.

L. Marsso, R. Mateescu, and Olivier Clozeau (Innovista Sensors) participated to the "*Forum 5i*" held on June 1st, 2017 at Grenoble (World Trade Center), where they held a stand dedicated to the results of the Bluesky project [0].

R. Mateescu gave a lecture entitled "*Validation d'applications embarquées par des jumeaux numériques formels*" at the *Journée thématique Minalogic sur la modélisation des systèmes cyber-physiques* held in Grenoble on November 16, 2017.

[0] http://projects.laas.fr/IFSE/FMF
[0] http://www.minalogic.com/en/project/bluesky

DEDUCTEAM Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Selection

8.1.1.1. Member of the Conference Program Committees

G. Burel was a member of the 12th International Workshop on the Implementation of Logics.

8.1.1.2. Reviewer

G. Burel, S. Martiel, and F. Gilbert rewiewed submissions to the Logic In Computer Science conference.

G. Burel reviewed submissions to the Formal Structures for Computation and Deduction conference.

8.1.2. Journal

8.1.2.1. Reviewer - Reviewing Activities

G. Burel reviewed articles for the Computer Journal and the Journal of Logic and Computation.

8.1.3. Invited Talks

G. Burel gave an invited lecture at the 28th Journées Francophones des Langages Applicatifs, entitled “Exprimer ses théories en Dedukti, le vérificateur de preuves universel”.

8.1.4. Scientific Expertise

G. Dowek is a member of the scientific concil of La Société Inforamatique de France.

G. Dowek is a member of the scientific concil of La Main à la Pâte.

G. Dowek is a member of the Commission de réflexion sur l’Éthique de la Recherche en sciences et technologies du Numérique d’Allistene.

8.1.5. Research Administration

F. Blanqui is co-director of the pole 4 (programming: models, algorithms, languages and architectures) of Paris-Saclay University’s doctoral school on computer science.

F. Blanqui is referent of LSV PhD students.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

F. Blanqui gave a M1 course (16h) on rewriting theory in the MPRI at the ENS Paris-Saclay.

F. Blanqui gave a M1 course (21h) on language theory at the ENSIIE.

G. Dowek’s paper *Rules and derivations in an elementary logic course* has been published in the IfCoLog Journal of Logics and their Applications [11].

8.2.2. Supervision

F. Blanqui supervised the internships of A. Defourné and R. Bocquet.

F. Blanqui and O. Hermant supervised the internship of G. Genestier.

F. Blanqui and O. Hermant supervise the PhD of G. Genestier.

G. Dowek supervises the PhD of G. Férey and F. Gilbert.

G. Dowek and D. Delahaye supervise the PhD of G. Bury.

G. Dowek and S. Graham-Lengrand supervise the PhD of F. Thiré.

8.2.3. Juries

F. Blanqui was member of the jury for the best scientific production of the year within Paris-Saclay University's doctoral school on computer science.

F. Blanqui has been in the jury for the PhD of R. Lepigre on "Semantics and Implementation of an Extension of ML for Proving Programs", Chambéry.

GALLIUM 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

Xavier Leroy participated in the program committee of the ACM symposium on Principles of Programming Languages (POPL 2018), of the European Symposium on Programming (ESOP 2018), and of the second Principles of Secure Compilation workshop (PRISC 2018).

Jean-Marie Madiot was a member of the program committee of the Interaction and Concurrency Experience Workshop (ICE 2017).

Michel Mauny was a member of the program committee for Trends in Functional Programming in Education (TFPIE 2017).

François Pottier was program chair of the ACM SIGPLAN Workshop on Higher-Order Programming with Effects (HOPE 2017) and a member of the program committee of the Journées Françaises des Langages Applicatifs (JFLA 2018).

Mike Rainey was a member of the program committee for the IEEE International Parallel and Distributed Processing Symposium (IPDPS 2018).

Didier Rémy was a member of the program commitee of the International Symposium on Functional and Logic Programming (FLOPS 2018).

10.1.2. Journal

10.1.2.1. Member of the Editorial Boards

Xavier Leroy is area editor (programming languages) for Journal of the ACM. He is a member of the editorial board of Journal of Automated Reasoning. Until June 2017, he was on the editorial board for the Research Highlights column of Communications of the ACM.

Michel Mauny is a member of the steering committee of the OCaml workshop.

François Pottier is a member of the ICFP steering committee and a member of the editorial boards of the Journal of Functional Programming and the Proceedings of the ACM on Programming Languages.

Didier Rémy is a member of the steering committee of the ML Family workshop.

10.1.3. Research Administration

Until September 2017, Xavier Leroy was an appointed member of Inria's *Commission d'Évaluation*. He participated in the following Inria hiring committees: *jury d'admissibilité DR2* and *jury d'admissibilité CR1*.

François Pottier is a member of Inria Paris' *Commission de Développement Technologique* and the president of Inria Paris' *Comité de Suivi Doctoral*.

Didier Rémy is *Deputy Scientific Director* (ADS) in charge of *Algorithmics, Programming, Software and Architecture*.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Didier Rémy is Inria's delegate in the pedagogical team of the MPRI (*Master Parisien de Recherche en Informatique*).

Master: Luc Maranget, "Semantics, languages and algorithms for multi-core programming", 18 HETD, M2 (MPRI), Université Paris Diderot, France.

Master: Michel Mauny, "Principles of Programming Languages", 32 HETD, M1, ENSTA-ParisTech, France.

Master: François Pottier and Didier Rémy, "Functional programming and type systems", 18 + 18 HETD, M2 (MPRI), Université Paris Diderot, France.

Licence: Armaël Guéneau, "Initiation à la programmation" (TP), "Projet informatique" (TP), "Concepts informatiques" (TD), "Langages et automates" (TD), 64 HETD, L1 and L2, Université Paris Diderot, France.

Licence: Thomas Williams, "Projet informatique" (TD), "Programation orientée objet et interfaces graphiques" (TD/TP), 64 HETD, L2, Université Paris Diderot, France.

10.2.2. Supervision

M1: Danny Willems, Université de Mons, supervised by 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: Pierrick Couderc (ENSTA-ParisTech & OCamlPro), "Typage modulaire du langage intermédiaire du compilateur OCaml," Université Paris-Saclay, since December 2014, supervised by Michel Mauny, Grégoire Henry (OCamlPro) and Fabrice Le Fessant.

PhD in progress: Albin Coquereau (ENSTA-ParisTech), "Amélioration de performances pour le solveur SMT Alt-Ergo: conception d'outils d'analyse, optimisations et structures de données efficaces pour OCaml," Université Paris-Saclay, since October 2015, supervised by Michel Mauny, Sylvain Conchon (LRI, Université Paris-Sud) and Fabrice Le Fessant.

PhD in progress: Armaël Guéneau, "Towards Machine-Checked Time Complexity Analyses", Université Paris Diderot, since September 2016, supervised by Arthur Charguéraud and François Pottier.

PhD in progress: Naomi Testard, "Reasoning about Effect Handlers and Cooperative Concurrency", Université Paris Diderot, since January 2017, supervised by François Pottier.

PhD in progress: Thomas Williams, "Putting Ornaments into practice", Université Paris Diderot, since September 2014, supervised by Didier Rémy.

10.2.3. Juries

Xavier Leroy was on the Ph.D. committees of Quentin Carbonneaux (Yale University, August 2017) and of Gabriel Radanne (University Paris Diderot, November 2017).

François Pottier was a reviewer for the Ph.D. thesis of Sandro Stucki (École Polytechnique Fédérale de Lausanne, September 2017). He was a member of the jury for the GDR GPL dissertation award (*prix de thèse du GDR GPL*).

10.3. Popularization

Xavier Leroy wrote a popularization article describing the hunt for a hardware bug in Intel processors, which was published by the Web news site *The Next Web* [32].

MARELLE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Member of the Organizing Committees

- Anders Mörtberg was an organizer of the 3rd workshop on Homotopy Type Theory and Univalent Foundations in Oxford, 8-9 September.

8.1.1.2. Chair of Conference Program Committees

- Yves Bertot was program committee co-chair for CPP'17 (Certified Programs and Proofs), in Paris, in January 2017.
- Yves Bertot is program committee co-chair for CoqPL'18 (Coq for Programming Lanugages), in Los Angeles, in January 2018.

8.1.1.3. Member of the Conference Program Committees

- Laurence Rideau was member of the program committee for JFLA'2018 (Journées francophones des langages applicatifs).

8.1.1.4. Reviewer

- Members of the team reviewed papers for JFLA (Journées Francophones des Langages Applicatifs), PoPL (Principles of Programming Languages), CPP (Certified Programs and Proofs), ITP (Interactive Theorem Proving), LPAR (Logic for Programming, Artificial Inteligence, and Reasoning), TACAS (Tools and Algorithms for the Construction and Analysis of Systems).

8.1.2. Journal

8.1.2.1. Reviewer - Reviewing Activities

- Members of the team reviewed papers for JAR (Journal of Automated Reasoning), and MSCS (Mathematical Structures in Computer Science).

8.1.3. Invited Talks

- Anders Mörtberg gave an invited talk at TTT (Type-Theory based Tools) in Paris in January and an invited talk at the workshop on Syntax and Semantics of Type Theory in Ljubljana in February.
- Cyril Cohen was invited for a talk at the workshop on Real Verification in South Korea in July.
- Damien Rouhling gave an invited talk at a meeting of the ANR-funded FastRelax project.

8.1.4. Scientific Expertise

- Yves Bertot performed a project review for the Dutch research funding agency (NWO).

8.1.5. Research Administration

- Yves Bertot is a member of the "Bureau du comité des projets".
- Yves Bertot is a member of the scientific committee for Academy "RISE" of University Côte d'azur.
- Yves Bertot was a member of the national working group for the strategic plan of Inria.
- Benjamin Grégoire is a member of the committee on the computer tool usage (CUMI) for the Sophia-Antipolis Méditerranée Inria center.
- José Grimm is a member of the local committee for hygiene and work safety.

- Laurence Rideau was a member of the Jury for hiring new researchers at Inria Sophia Antipolis (Jury d’admissibilité de chargés de recherche, Inria Sophia Antipolis Méditerranée).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Doctorat: Enrico Tassi organized an advanced school on Coq and the Mathematical Components library, where Laurence Rideau, Cyril Cohen, Laurent Théry, and Yves Bertot gave lectures and supervised laboratory sessions. This school took place in December and had 12 attendants.

Doctorat: Enrico gave a course "Type Theory, The Coq proof assistant", at the University of Padova in June.

Master: Yves Bertot organized an introductory school on Coq. This school took place in January and had 12 attendants.

Licence: Sophie Bernard gave 54 hours of lectures on probabilities at University of Nice Sophia Antipolis.

Licence: Damien Rouhling taught about 60 hours at University Nice Sophia Antipolis: differential calculus, Fourier analysis, and C programming (First year students).

Licence: Boris Djalal taught 4 hours of computer science for first year students in a "classe préparatoire aux grandes écoles".

Licence: Cécile Baritel-Ruet taught 30 hours of computer science for first year students at Université de Nice, and 12 hours of lectures on computer science history.

Licence: Laurence Rideau taught 10 hours of computer science in a "classe préparatoire aux grandes écoles"

Licence: Cyril Cohen gives mathematics exercises in a "classe préparatoire aux grandes écoles".

Master: Laurent Théry taught 3 hours on "introduction to computer verified proof" at Ecole des Mines de Paris,

8.2.2. Supervision

PhD in progress : Cécile Baritel-Ruet, "Formal verification of Security with EasyCrypt", started October 2016, supervised by Benjamin Grégoire and Yves Bertot,

PhD in progress : Sophie Bernard, "Formal proofs for transcendance", started October 2016, supervised by Yves Bertot and Laurence Rideau,

PhD in progress : Boris Djalal, "Formal verification of cylindrical algebraic decomposition", supervised by Cyril Cohen and Yves Bertot,

PhD in progress : Mohammad El Laz, "Formal study of Security", started December 2017, supervised by Benjamin Grégoire and Tamara Rezk (Indes Inria project team),

PhD in progress, : Damien Rouhling, "Formal proofs for control and robotics", started in October 2016, supervised by Yves Bertot and Cyril Cohen.

8.2.3. Juries

- Laurent Théry attended the middle thesis review for David Braun, in Strasbourg,
- Enrico Tassi was a member of the Jury for the defence of Roberto Blanco Martinez (Ecole Polytechnique),
- Laurent Théry was a member of the Jury for the defence of Thomas Sibut-Pinote (Ecole Polytechnique).

8.3. Popularization

Laurent Théry gave a talk in high-school (Centre International de Valbonne) in the context of the annual "Fête de la Science".

Damien Rouhling and Cécile Baritel-Ruet participated to the event "My thesis in 180 seconds" at the regional level.

MEXICO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Matthias Függer is general co-chair of *ASYNC 2018*

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Laurent Fribourg was a PC member of:
  - 7th International Conference on New Computational Methods for Inverse Problems, Cachan, 2017
  - The 27th International Symposium on Logic-based Program Synthesis and Transformation, Namur, Belgium, 2017
  - Seventh Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, Seoul, 2017.
- Matthias Függer was a member of the PC of DDECS'17.
- Stefan Haar was a member of the PCs of the conferences MSR 2017 and *ACSD 2017* and of the workshop *ATAED 2017*.
- Serge Haddad was a PC member of the *International Workshop on Petri Nets and Software Engineering* (PNSE) 2017 at Zaragoza, Spain, and of the *11th International Conference on Verification and Evaluation of Computer and Communication Systems* (VECOS) 2017 at Montreal, Québec, Canada. He was also a member of the scientific committee of *Ecole d'été temps-réel* (ETR 2017).

9.1.2.2. Reviewer

- Matthias Függer was a reviewer for ICALP, DISC, FMCAD, ICDCN,and OPODIS.
- Stefan Haar was a reviewer for FOSSACS.
- Stefan Schwoon was a reviewer for the following conferences taking place in 2017: STACS, TACAS, ESOP, ATVA, and FSTTCS.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Stefan Haar is associate editor of the *Journal of Discrete Event Dynamic Systems: Theory and Applications*.

9.1.3.2. Reviewer - Reviewing Activities

- Thomas Chatain was a reviewer for Acta Informatica, Artificial Intelligence and Journal of Discrete Event Dynamic Systems.
- Matthias Függer was a reviewer for MFCS.
- Stefan Haar was a reviewer for MSCS and IEEE Transations on Automatic Control.
- Stefan Schwoon was a reviewer for Fundamenta Informaticae, International Journal on Software Tools for Technology Transfer, and the Journal of Discrete Event Dynamic Systems.

9.1.4. Invited Talks

- Laurent Fribourg gave the following invited talk: "Euler's Method Applied to the Control of Switched Systems", at 15th International Conference on Formal Modelling and Analysis of Timed Systems, Berlin, 2017
- Matthias Függer gave invited talks at the Theory of Hardware seminar in Vienna in February, the Noon seminar at Max-Planck Institute for Informatics in April, and the Distributed Computing Seminar at Labri in November.
- Serge Haddad gave the following invited talks:
  - at Centre Fédéré en Vérification, Bruxelles, Belgique on February 24, 2017, entitled *From Continuous Petri nets to Petri nets and Back*;
  - at LACL, Créteil on February 27, 2017, entitled *Probabilistic Disclosure: Maximisation vs. Minimisation*
  - at the MSR 2017 conference, Marseille, France, on November 16, 2017, entitled *Réseaux de Petri discrets et continus : apports réciproques*.
- Claudine Picaronny gave an invited talk on 'Vérification probabiliste, numérique ou statistique', on the 21th of april 2017 at Alea 17, CIRM Marseille, France

9.1.5. Scientific Expertise

- Serge Haddad was expert for the evaluation of the researcher premiums at University Pierre et Marie Curie

9.1.6. Research Administration

- Laurent Fribourg is a member of
  - Comité Direction of Department Sciences et technologies de l'information et de la communication of Université Paris-Saclay,
  - Bureau of Domaine d'Intérêt Majeur émergent du Réseau Francilien en Sciences Informatiques
- Stefan Haar is the president of Inria's *GTRI-COST* committee for international relations, and the head of the SciLex (Software Reliability and Security) axis of the *LABEX*DIGICOSME, and ipso facto a member of *DIGICOSME*'s executive committee and scientific commission.
- Serge Haddad was the president of the HCERES evaluation committee of the laboratory LIAS, Poitiers.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Stefan Haar taught one half of L3 level class on Formal Languages at ENS Paris-Saclay (15 h CM, 22.5 EQTD).
- Serge Haddad is professor at ENS Paris-Saclay. Claudine Picaronny, Thomas Chatain, and Stefan Schwoon are associate professors of the same university.
- Serge Haddad is the head of the Computer Science Department, and Stefan Schwoon is in charge of the L3 formation.
- Claudine Picaronny is a co-director of the ENS Paris-Saclay's Mathematics department and a member of the juries of the 'agrégation interne de Mathématiques' and of the second 'concours de Mathématiques' of ENS Paris-Saclay; she is also the coordinator of the mathematics/computer science examination of E3A, parts MP and MC.
- Matthias Függer is teaching "Initiation à la recherche" at ENS Paris-Saclay.

9.2.2. Supervision

Theses in progress:

Hugues Mandon, ENS Paris-Saclay since October 2016, on *computational models and algorithms for the prediction of Cell Reprogramming Strategies*, co-supervised by Stefan Haar and L. Paulevé (LRI)

Juraj Kolcˇák, , ENS Paris-Saclay since March 2017, on *Unfoldings and Abstract Interpretation for Parametric Biological Regulatory Networks*, co-supervised by Stefan Haar and L. Paulevé (LRI).

Adnane Saoud, Université Paris-Saclay since 2016, jointly supervised by Laurent Fribourg and Antoine Girard (Centrale-Supelec).

Engel Lefaucheux, ENS Paris-Saclay since 2015, *Controlling information in probabilistic systems*, jointly supervised by Nathalie Bertrand (SUMO team) and Serge Haddad

Yann Duplouy, IRT SystemX since 2015, *Application of formal methods to the development of embedded systems for autonomous vehicles*, supervised by Béatrice Bérard and Serge Haddad.

Robert Najvirt (TU Wien, Austrian FWF SIC project), realistic delay models with applica- tions in high-speed and low-power circuits, co-supervised by Matthias Függer and Andreas Steininger.

Martin Perner (TU Wien, Austrian FWF SIC project), clock generation on-chip and formalisms suitable to prove correct VLSI circuits, co-supervised by Matthias Függer and Ulrich Schmid.

Juergen Maier (TU Wien, Austrian FWF SIC project), on realistic delay models with applications in high-speed and low-power circuits, with focus on noise and high-order models, co-supervised by Matthias Függer and with Ulrich Schmid.

9.2.3. Juries

- Laurent Fribourg was a member of the Jury of Irini-Eleftheria Mens's PhD Thesis on “Learning regular languages over large alphabets", defended at University of Grenoble, October 2017.
- Stefan Haar was a reviewer of the thesis by Guillaume Madelaine on 'Simplifications Exactes et Structurelles de Réseaux de Réactions Biologiques', defended on February 28 at Lille University, France.
- Serge Haddad was:
  - reviewer in the jury of Bruno Karelovic on *Quantitative Analysis of Stochastic Systems – Priority Games and Populations of Markov Chains* on July 7 2017, University Paris 7
  - president of the jury of Nicolas David on *Réseaux de Petri à Paramètres Discrets* on October 20 University Nantes
  - reviewer in the jury of Thomas Geffroy on *Vers des outils efficaces pour la vérification de systèmes concurrents* on December 12 2017, University Bordeaux
- Claudine Picaronny was Member of the jury of Pierre Carlier's Thesis on 'Verification of Stochastic Timed Automata', on the 8th of december 2017, Mons, Belgium

PARSIFAL Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

D. Miller has been selected to be the LICS General Chair for three years starting in July 2018.

8.1.1.2. Member of the Organizing Committees

Lutz Straßburger was member of the organizing committee for the second FISP meeting in Paris

8.1.2. Scientific Events Selection

8.1.2.1. Chair of Conference Program Committees

D. Miller was the Program Committee chair for the FSCD'17: Second International Conference on Formal Structures for Computation and Deduction, Oxford, 3-6 September.

D. Miller was on the Steering Committee for the FSCD series of International Conference on Formal Structures for Computation and Deduction.

D. Miller was a member of the jury for selecting the 2017 Ackermann Award (the EACSL award for outstanding doctoral dissertation in the field of Logic in Computer Science).

D. Miller was a member of the 2012, 2016, and 2017 Herbrand Award Committee of the Association for Automated Reasoning.

D. Miller is also a member of the SIGLOG advisory board, starting November 2015.

B. Accattoli was one of the two Program Committee chairs of the 6th International Workshop on Confluence (IWC 2017).

K. Chaudhuri as a co-chair of the Program Committee for the workshop on Structures and Deduction, co-located with FSCD.

8.1.2.2. Member of the Conference Program Committees

D. Miller was on the Program Committee of the following international conferences.

- 26th International Conference on Automated Deduction, Gothenburg, Sweden, 6-11 August.

B. Accattoli was on the Program Committee of the following international workshops.

- LOLA 2017: Syntax and Semantics of Low-Level Languages, Reykjavik, Iceland, 19 June.
- WPTE 2017: 4th Workshop on Rewriting Techniques for Program Transformations and Evaluation, Oxford, UK, 8 September.
- DICE-FOPARA 2017: 8th Workshop on Developments in Implicit Computational complExity and 5th Workshop on Foundational and Practical Aspects of Resource Analysis, Uppsala, Sweden, 22–23 April.

S. Graham-Lengrand was on the Program Committee of the following international workshops.

- AFM 2017: Automated Formal Methods, Menlo Park, USA, 19 May.
- PxTP 2017: 5th Workshop on Proof eXchange for Theorem Proving, Brasilia, Brazil, 4 September.

K. Chaudhuri was on the Program Committee of the following international workshops.

- LFMTP 2017: Logical Frameworks and Meta-languages: Theory and Practice, Oxford, U.K.
- LSFA 2017: Logical and Semantic Frameworks with Applications, Brasilia, Brazil

G. Scherer was on the Program Committee of the following international conference.

- Trends in Functional Programming, University of Kent at Canterbury, UK, 19-21 June.

8.1.2.3. Reviewer

- Lutz Straßburger reviewed submissions for the following conferences: LICS 2017, LPAR-21, FoSSaCS 2018, LFCS 2018
- B. Accattoli was a reviewer for the international conferences LICS 2017 (twice) and FSCD 2017.
- F. Lamarche was reviewer for CSL 2017.
- S. Graham-Lengrand was a reviewer for the international conferences LICS 2017 (three times), CADE 2017, AFM 2017, CSL 2017, TYPES 2017, PxTP 2017, FOSSACS 2018.
- G. Scherer reviewed submissions for the following conferences: JFLA 2018, FoSSaCS 2018, as well as for the PriSC 2018 (Principle of Secure Compilation) workshop.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

D. Miller is on the editorial board of the following journals: ACM Transactions on Computational Logic, Journal of Automated Reasoning (Springer), and Journal of Applied Logic (Elsevier).

K. Chaudhuri served as a guest editor for a special issue of Mathematical Structures of Computer Science devoted to Logical Frameworks.

8.1.3.2. Reviewer - Reviewing Activities

- Lutz Straßburger did reviewing work for the following journals: Journal of Applied Logic (JAL), Studia Logica, Mathematical Structures in Computer Science (MSCS), Logical Methods in Computer Science (LMCS), Journal of Logic and Computation (JLC), Journal of Automated Reasoning (JAR).
- B. Accattoli was a reviewer for the international journals Transactions on Computational Logic (TOCL, ACM), Mathematical Structures in Computer Science (MSCS, Cambridge University Press), Logical Methods in Computer Science (LMCS), Journal of Automated Reasoning (JAR, Springer), Annals of Pure and Applied Logic (APAL, Elsevier).
- S. Graham-Lengrand was a reviewer for the following international journals: Theory of Computing Systems (TOCS), Annals of Pure and Applied Logic (APAL), Mathematical Structures in Computer Science (MSCS), Logical Methods in Computer Science (LMCS), Journal of Automated Reasoning (JAR), Bulletin of Symbolic Logic (BSL).
- G. Scherer was a reviewer for the international journal Mathematical Structures in Computer Science (MSCS).

8.1.4. Invited Talks

- D. Miller gave invited talks at the following two regularly held international meetings.
  - LAP 2017: Sixth Conference on Logic and Applications, 18-22 September 2018, Dubrovnik, Croatia.
  - PADL 2017: Nineteenth International Symposium on Practical Aspects of Declarative Languages, 16-17 January 2017, Paris.
- Lutz Straßburger gave an invited talk at the 4th International Workshop on Structures and Deduction (SD 2017), affiliated with FSCD'17.
- B. Accattoli gave an invited talk at LSFA 2017, the 12th Workshop on Logical and Semantic Frameworks with Applications, Brasilia, Brazil, 23-24 September.
- S. Graham-Lengrand gave an invited talk at CSLI 2017, the 6th CSLI Workshop on Logic, Rationality & Intelligent Interaction, University of Stanford, Palo Alto, USA, 3-4 June.

8.1.5. Research Administration

L. Straßburger serves on the “commission développement technologique (CDT)” for Inria Saclay–Île-de-France (since June 2012).

F. Lamarche was “responsable de centre” Saclay – Ile de France for Raweb.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master: D. Miller, “*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*”, 12 hours, M2, Master Parisien de Recherche en Informatique, France.

Lutz Straßburger gave a course on “Efficient Proof Systems for Modal Logics” at ESSLLI 2017 (joint with Roman Kuznets, TU Wien)

Master: B. Accattoli, “*MPRI 2-1: Logique linéaire et paradigmes logiques du calcul*”, 9 hours, M2, Master Parisien de Recherche en Informatique, France.

B. Accattoli taught the mini-course *the complexity of β-reduction*, 3 hours, at the International School on Rewriting 2017, Eindhoven, The Netherlands, 3-7 July.

Licence: S. Graham-Lengrand, “*INF412: Fondements de l’Informatique: Logique, Modèles, Calcul*”, 32 hours eq. TD, L3, École Polytechnique, France.

Master: S. Graham-Lengrand, “*INF551: Computational Logic*”, 45 hours eq. TD, M1, École Polytechnique, France.

Licence: K. Chaudhuri, “*INF431*: Concurrence” and “*INF441*: Programmation avancée”, 80 hours eq. TD, L2, Ecole polytechnique, France.

8.2.2. Supervision

PhD in progress: Sonia Marin, 1 Nov 2014, supervised by L. Straßburger and D. Miller

PhD in progress: Roberto Blanco, Ulysse Gérard, and Matteo Manighetti, supervised by D. Miller

PhD in progress: François Thiré (since 1st October 2016), supervised by S. Graham-Lengrand (joint with G. Dowek)

8.2.3. Juries

D. Miller was a reporter for the habilitation of Olivier Hermant, 20 April 2017.

PI.R2 Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Pierre-Louis Curien is organising a Day of Hommage to the memory of Maurice Nivat on Fevruary 6, 2018, at University Paris 7.

8.1.1.2. Member of the Organising Committees

Yann Régis-Gianas was multimedia chair of the organising committee of POPL 2017 that took place in Paris in January 2017.

Yves Guiraud, Philippe Malbos and Samuel Mimram have organised the third edition of the Higher-Dimensional Rewriting and Algebra (HDRA) workshop of the Formal Structures for Computation and Deduction conference (FSCD), held in Oxford in September 2017.

Yves Guiraud and Samuel Mimram, with Dimitri Ara (Univ. Aix-Marseille) have organised the "Categories in Homotopy and Rewriting" one-week international conference, at the CIRM, in Marseille, in September 2017. As the closing conference of the Cathre ANR project, focused on higher-dimensional algebra, this conference attracted 80 participants, working in category theory, algebraic topology, logic and theoretical computer science.

Matthieu Sozeau co-organised with Nicolas Tabareau the 3rd Coq Implementors Workshop in Le Croisic, France, June 12-16 2017. It included presentations from developers, both from France and abroad and a large amount of hacking.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

Hugo Herbelin was a member of the program committees of the conference FSCD'17, of the TYPES'17 venue, as well as of the PxTP'17 and CoqPL'18 workshops.

Matthieu Sozeau was member of the program committee of CoqPL'17.

Yann Régis-Gianas was member of the program committee of JFLA'18.

Alexis Saurin was a member of the program committee of the workshop Coinduction in Type Theory which took place in Chambéry from the 3rd to the 6th of July, 2017

Alexis Saurin was a member of the program committee of the workshop on Trends in Linear Logic and Applications which took place in Oxford on the 3rd of September 2017 as a satellite event of FSCD conference.

8.1.2.2. Member of the Conference Steering Committees

Hugo Herbelin was a member of the steering committee of the conference *Formal Structures for Computation and Deduction* (FSCD) until September 2017.

Hugo Herbelin is a member of the steering committee of the conference *TYPES*.

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).

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

Pierre-Louis Curien is editor in chief of the Cambridge University Press journal Mathematical Structures in Computer Science (since January 2016).

Alexis Saurin is editing a special issue of MSCS dedicated to contributions in honour of Dale Miller for his 60th birthday.

8.1.3.2. Reviewer - Reviewing Activities

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

8.1.4. Invited Talks

Pierre-Louis Curien gave an invited talk at the Conference Categories for Homotopy Theory and Rewriting on “A syntactic approach to polynomial functors, polynomial monads and opetopes” (September 2017).

Yann Régis-Gianas gave an invited talk at the Conference for Trends in Functional Programming In Education on the OCaml MOOC (April 2017).

8.1.5. Scientific Expertise

Pierre-Louis Curien and Yves Guiraud have been members of the “Comité de sélection” for an assistant professor position in mathematical foundations of computer science at the University Paris 7 (spring 2017).

8.1.6. Research Administration

Pierre-Louis Curien, Hugo Herbelin and Yves Guiraud are members of the scientific council of the Computer Science deparment of University Paris 7.

Yves Guiraud is the head of the “Preuves, Programmes and Systèmes (PPS)” pole of the IRIF laboratory (since April 2016), a member of the IRIF council (January 2016 - December 2017), and of the IRIF direction council (since September 2017).

Pierre-Louis Curien is a member of the Scientific Council of the CIRM (Centre International de Rencontres Mathématiques.

8.1.7. Presentation of papers

Hugo Herbelin gave a talk at the GT Geocal-Lac on a proof of Gödel’s completeness theorem using side-effects.

Hugo Herbelin gave a talk at the PPS pole days on the intuitionistic reverse mathematics properties of Gödel’s completeness theorem.

Étienne Miquey gave a talk at the ESOP conference in Uppsala (Sweden) on “A classical sequent calculus with dependent types” (April 2017).

Jovana Obradović gave a talk at the Conference Topology in Ecuador (Galapagos Islands) on “Categorified cyclic operads” (August 2017).

Théo Zimmermann gave a talk on Coq’s Prolog and application to defining semi-automatic tactics at the TTT’17 workshop (Type-Theory Based Tools).

Cyprien Mangin gave a talk on Equations at the TTT’17 workshop.

Matthieu Sozeau gave a talk on Coq 8.6 at the CoqPL’17 workshop in January 2017.

8.1.8. Talks in seminars

Pierre-Louis Curien gave talks at NII (Hasuo’s Lab, Tokyo) and at Shanghai Jiaotong University on “Trialgebraic structures on faces of some families of polytopes” (October-November 2017).

Théo Zimmermann gave a talk on transfer of isomorphisms at the Deducteam seminar (April 2017).

8.1.9. Attendance to conferences, workshops, schools,...

Hugo Herbelin attended TTT'17, TYPES'17 and FSCD'17.

Cyrille Chenavier, Maxime Lucas, Philippe Malbos and Samuel Mimram attended the HDRA workshop in Oxford (September 2017).

Cyrille Chenavier, Pierre-Louis Curien, Yves Guiraud, Maxime Lucas, Philippe Malbos and Samuel Mimram attended the "Categories in Homotopy and Rewriting" conference in Marseille (September 2017).

Hugo Herbelin attended the conferences Types 2017 in Budapest (Hungaria, May), the Coq implementors workshop in Le Croisic (June), the FSCD conference in Oxford (UK, September). He attended various workshops of the POPL'17 and FSCD'17 conference, including TTT'17 and CoqPL'17. He participated to the Big Proofs seminar in Cambridge (July).

Jean-Jacques Lévy participated to CAV and VSTTE 2017 conferences, Heidelberg, Germany, July 21-28 where his co-author Ran Chen presented the article [36].

Matthieu Sozeau attended POPL'17, CPP'17 and CoqPL'17 in Paris (January), TYPES'17 in Budapest (Hungaria, May) and the Coq implementors workshop in Le Croisic (June).

Étienne Miquey attended the conference ESOP in Uppsala (Sweden) in April 2017.

Pierre-Louis Curien and Jovana Obradović attended the conference Topology in Ecuador (Galapagos Islands) in August 2017, and the conference Geometry and combinatorics of associativity in Dublin in October 2017.

Pierre-Louis Curien and Claudia Faggian attended the CRECOGI meeting in Ito (Japan), and Claudia Faggian gave a talk on "Proof techniques in Probabilistic Reduction Systems" (November 2017).

Théo Zimmermann attended the TTT'17 workshop (January 2017) and the Coq implementors workshop in Le Croisic (June 2017).

8.1.10. Groupe de travail Théorie des types et réalisabilité

This is one of the working groups of PPS, jointly organised by Hugo Herbelin and Matthieu Sozeau.

The speakers in 2017 were Pierre-Marie Pédrot, Guilhem Jaber, Francesco A. Genco, Ludovic Patey.

8.1.11. Groupe de travail Catégories supérieures, polygraphes et homotopie

Several members of the team participate actively in this weekly working group of PPS, organised by François Métayer (IRIF) since 2009.

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).

Master: Hugo Herbelin teaches the course on the proof-as-program correspondence for classical logic and beyond at the LMFI.

Master: Pierre Letouzey teaches two short courses to the LMFI Master 2 students : "Models of programming" and "Introduction to computed-aided formal proofs". These two courses come in addition to Pierre Letouzey's regular duty as teacher in the Computer Science department of Paris 7 (including a course on Compilation to M2-Pro students).

Master: Yves Guiraud gave a course on the applications of rewriting methods in algebra in the M2 Mathématiques Fondamentales of Lyon (Univ. Lyon 1 and ENS Lyon).

Master: Matthieu Sozeau taught the MPRI course on Advanced uses of proof assistants (12 hours + a project), together with Bruno Barras (Inria Deducteam).

Matthieu Sozeau taught a course at the EJCP'17 summer school in Toulous in June 17, on an introduction to interactive theorem proving.

Master: Alexis aurin taught the proof theory and lambda-calculus part of the cours fondamental de logique in M2 "Logique Mathématique et Fondements de l'Informatique", Université Paris 7.

Alexis Saurin chairs LMFI M2 since September 2013.

8.2.2. Supervision

Internship: Hugo Herbelin has supervised the M2 internship of Charlotte Barot.

Internship: Yann Régis-Gianas has supervised the L3 internship of Kostia Chardonnet.

Internship: Yann Régis-Gianas has supervised the M2 internship of Colin Gonzalez.

PhD (completed) Amina Doumane, supervised by Alexis Saurin, David Baelde and Pierre-Louis Curien, successfully defended in June 2017 (title: On the infinitary proof theory of logics with fixed points).

PhD (completed): Étienne Miquey, co-supervised by Hugo Herbelin and Alexandre Miquel, Réalisabilité classique et effets de bords, September 2014, successfully defended in November 2017.

PhD (completed): Jovana Obradović, supervised by Pierre-Louis Curien, successfully defended in Septemver 2017 (title: Cyclic operads: syntactic, algebraic and categorified aspects).

PhD (completed): Maxime Lucas, supervised by Yves Guiraud and Pierre-Louis Curien, successfully defended in December 2017 (title: Cubical categories for homotopy and rewriting).

PhD in progress: Guillaume Claret, Programmation avec effets en Coq, (started in September 2012), supervised by Hugo Herbelin and Yann Régis-Gianas, the dissertation was completed in 2015 but Guillaume Claret moved in the meantime to a private company and the defense has been delayed to 2018.

PhD in progress: Thibaut Girka, Differential semantics (started in January 2014), supervised by Roberto Di Cosmo and Yann Régis-Gianas.

PhD in progress: Cyprien Mangin, Dependent Pattern-Matching, induction-induction and higher inductive types (started in September 2015), supervised by Matthieu Sozeau and Bruno Barras

PhD in progress: Théo Zimmermann (started in September 2016), supervised by Hugo Herbelin.

PhD starting: Cédric Ho Thanh, on Opetopes for higher-dimensional rewriting and koszulity, supervised by Pierre-Louis Curien and Samuel Mimram.

The following are cosupervisions of PhD students who are not formally part of the team:

PhD in progress: Rémi Nollet, Functional reactive programming and temporal logics: their syntax and semantics - from discrete to continuous time (started in September 2016), supervised by Alexis Saurin and Christine Tasson.

PhD in progress: Gaëtan Gilbert (at Inria Nantes), Definitional proof-irrelevance in the Calculus of Inductive Constructions (started in September 2016), supervised by Nicolas Tabareau and Matthieu Sozeau.

PhD in progress: Simon Forest (at École Polytechnique), Rewriting in semistrict higher categories (started in September 2017), supervised by Samuel Mimram and Yves Guiraud.

PhD in progress: Théo Winterhalter (at Inria Nantes), Extensional to Intensional type theory and meta-theory of proof-irrelevance (started in September 2017), supervised by Nicolas Tabareau and Matthieu Sozeau.

8.2.3. Juries

Pierre-Louis Curien was referee for the Habilitation of Russ Harmer (ENS Lyon, May 2017).

Pierre-Louis Curien and Alexis Saurin were members of the jury of the thesis of Amina Doumane (Paris 7, June 2017).

Pierre-Louis Curien was president of the jury of the Habilitation of Matthieu Picantin (Paris 7, July 2017).

Pierre-Louis Curien was president of the jury of the thesis of Simon Castellan (ENS Lyon, July 2017).

Pierre-Louis Curien was member of the jury of the thesis of Jovana Obradović (Paris 7, September 2017).

Pierre-Louis Curien was referee for the Habilitation of Paul-André Melliès (Paris 7, November 2017).

Pierre-Louis Curien was president of the jury of Habilitation of Damiano Mazza (Paris 13, December 2017).

Pierre-Louis Curien was referee for the Habilitation of Samuele Giraudo (Marne la Vallée, December 2017).

Pierre-Louis Curien was member of the jury of the thesis of Nicolas Ninin (Paris Saclay, December 2017).

Pierre-Louis Curien was president of the jury of the thesis of Luc Pellissier (Paris 13, December 2017).

Pierre-Louis Curien was referee for the thesis of Christopher Nguyen (Macquarie University, Sydney, December 2017).

Pierre-Louis Curien and Yves Guiraud were members of the jury of the thesis of Maxime Lucas (Paris 7, December 2017).

8.3. Popularization

Hugo Herbelin wrote with Sandrine Blazy and Pierre Castéran an introduction to Coq for engineers edited by Techniques de l'Ingénieur.

SUMO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Éric Badouel was the scientific chair of CRI 2017.
- Hervé Marchand is member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. Hervé Marchand is member of the steering committee of MSR (modélisation de systèmes réactifs) since 2012 and became president of this steering in November 2017;
- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the Summer School MOVEP ("*Modelisation et Vérification des Processus Parallèles*").

10.1.1.2. Member of the Organizing Committees

- Thierry Jéron is member of the steering committee of FMF 2017 (Formal Methods Forum), a forum gathering people from academia and industry and dedicated to the use of formal methods. It is held in Toulouse and, since this year, retransmitted in Grenoble, Saclay and Rennes. Two sessions took place in 2017, in January on the theme "Formal methods and cybersecurity" and in October about "Autonomous vehicles and formal methods".

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- Nathalie Bertrand was PC co-chair with Luca Bortolussi of QEST'2017, the 14th International Conference on Quantitative Evaluation of Systems, held in Berlin in September 2017 [45].

10.1.2.2. Member of the Conference Program Committees

- Éric Badouel was member of the program committees of VECOS 2017, ATAED 2017 and CRI 2017.
- Nathalie Bertrand was member of the PC of the following conferences: LICS 2017, FCT 2017, MSR 2017.
- Blaise Genest was a PC member of ATVA 2017;
- Thierry Jéron served on the Program Committees of the following international conferences: SAC-SVT 2017 and SAC-SVT 2018.
- Hervé Marchand served on the Program Committees of MSR 2017, Wodes 2018, CDC 2017, CCTA 2017.
- Nicolas Markey was a PC member of ATVA 2017, FORMATS 2017, SR 2017.
- Ocan Sankur was a PC member of SR 2017 and SYNT 2017.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Éric Badouel is co-editor-in-Chief of ARIMA Journal.

10.1.4. Invited Talks

- Nathalie Bertrand was invited to give a talk at the workshop organized for the 20 years of LSV (ENS Cachan) in May 2017. She was also invited to talk at the workshop OPCT (Open Problems in Concurrency) in June 2017 at IST Vienna (Austria).
- Hervé Marchand gave an invited talk during the conference of MSR (November 2017) titled *Contribution to the Analysis of Discrete Event Systems* as well as during the workshop “30 years of the Ramadge-Wonham Theory of Supervisory Control: A Retrospective and Future Perspectives” at the CDC conference in December 2017 titled *Opacity and Supervisory Control*.
- Nicolas Markey gave an invited talk about *Temporal logics for multi-agent systems* at MFCS 2017, Aalborg (Denmark), in August 2017 [27].

10.1.5. Leadership within the Scientific Community

- Since September 2017, Nathalie Bertrand is, together with Pierre-Alain Reynier, co-head of the *Groupe de Travail Verif* belonging to the *GDR Informatique Mathématique* (GDR-IM).

10.1.6. Research Administration

- Éric Badouel is the co-director (with Moussa Lo, UGB, Saint-Louis du Sénégal) of LIRIMA, the Inria International Lab for Africa. He is scientific officer for the African and Middle-East region at Inria European and International Partnership Department and member of the executive board of GIS SARIMA.
- Nathalie Bertrand is elected member of the *Conseil National des Universités*, section 27 (computer science).
- Nathalie Bertrand, Loïc Hélouët and Ocan Sankur organize the weekly seminar 68NQRT at IRISA (40 talks each year).
- Éric Fabre is the co-director (with Olivier Audouin, Nokia) of the joint lab of Nokia Bell Labs France and Inria. The lab has been running for 9 years and started in Nov. 2017 its 3rd phase of joint research teams. A series of 6 new teams just started, for a duration of 4 years. They cover topics like network virtualization, network management, information theory, (distributed) machine learning, network security. SUMO is involved in the joint team "Softwarization of Everything".
- Loïc Hélouët is a representative of rank-B researchers in the *Comité de Centre* of Inria Rennes. He is also part of the bureau of the Comité de Centre. He leads the P22 projects with Alstom transports and is responsible for Workpackage 2 of the Headwork ANR project.
- Thierry Jéron is Member Committee Substitute for COST IC1402 ARVI (Runtime Verification beyond Monitoring). He is member of the IFIP Working Group 10.2 on Embedded Systems. He is member of the COS Prospective of Irisa Rennes and member of the *Comité de Centre* of Inria Rennes. Since 2016 he is *référent chercheur* for the Inria-Rennes research center.
- Hervé Marchand is chairman of the CUMI in Rennes and member of the ADT commission in Rennes.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence: Nathalie Bertrand, Advanced Algorithms (ALGO2), 20h, L3, Univ Rennes 1, France;
- Licence: Loïc Hélouët, JAVA and algorithmics, L2, 40h, INSA de Rennes, France.
- Licence: Loïc Hélouët, practical studies (development of a small project), 8h, INSA de Rennes, France.
- Master : Nathalie Bertrand, Language Theory; Algorithms, 15h, Agrégation, ENS Rennes, France;
- Master: Éric Fabre, Models and Algorithms for Distributed Systems (MADS), 10h, M2, Univ Rennes 1, France;

- Master: Éric Fabre, Information Theory, 15h, M1, ENS Rennes, France.
- Master: Blaise Genest, Verification of Complex Systems (CSV), 10h, M2, Univ. Rennes 1, France;
- Master: Loïc Hélouët, Algorithms; complexity, 8h, Agrégation, ENS Rennes, France;
- Master: Loïc Hélouët, Nathalie Bertrand, Ocan Sankur, supervision of 3 students in M1 SIF (2017-2018).
- Master: Nicolas Markey, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;
- Master: Nicolas Markey, Algorithms for graphs, 3h, Agrégation, ENS Rennes, France;
- Master: Ocan Sankur, Lab sessions for the course on Foraml Analysis and Design (ACF), 22h, M1, Univ. Rennes 1, France.

10.2.2. Supervision

10.2.2.1. Defences

- HdR: Hervé Marchand, *Contribution to the Analysis of Discrete Event Systems* [15], Univ. Rennes 1. The defence took place on 6 June 2017.
- PhD: Bruno Karelovic, *Analyse quantitative des systèmes stochastiques – Jeux de priorité et population de chaînes de Markov*, Univ. Paris 7. The defence took place on 7 July 2017. Co-directed by Blaise Genest.

10.2.2.2. PhD in progress

- Robert Nsaibirni, *A Guarded Attribute Grammar Model for User centered Distibuted Collaborative Case Management: Case of the Disease Surveillance Process*, co-advised by Éric Badouel and Maurice Tchuenté (University of Yaoundé).
- Engel Lefaucheux, *Controlling information in probabilistic systems*, started September 2015, Nathalie Bertrand and Serge Haddad
- The Anh Pham, *Dynamic Formal Verification of High Performance Runtimes and Applications*, started Nov. 2016, Thierry Jéron and Martin Quinson (Myriads, Inria Rennes).
- Karim Kecir, *Régulation et robustesse des systèmes ferroviaires urbains*, planned May 2018, Loïc Hélouët and Pierre Dersin (Alstom).
- Hugo Bazille, *Information flows in quantitative dynamic systems*, started oct. 2016, Blaise Genest and Éric Fabre.
- Erij Elmajed, *Diagnosis of reconfigurable systems*, started March 2017, Éric Fabre and Armen Aghasaryan (Nokia).
- Sihem Cherrared, *Diagnosis of multi-tenant programmable networks*, started Dec. 2016, Éric Fabre, Gregor Goessler (Inria, Spades) and Sofiane Imadali (Orange).
- Victor Roussanaly, *Efficient verification of timed systems*, started Sep. 2017, Nicolas Markey and Ocan Sankur.

10.2.2.3. Master2 internship supervision

- Internship Aina Toky Rasoamanana, Feb-July 2017, Nathalie Bertrand and Nicolas Markey
- Internship Victor Roussanaly, Feb-June 2017, Nicolas Markey and Ocan Sankur

10.2.2.4. Other internship supervision

- L3 Internship of Balasubramanian A.R., May-July 2017, Nathalie Bertrand and Nicolas Markey
- L3 Internship of Thomas Mari, *Observation-based unfolding of Petri nets*, (May-July 2017)
- L3 Internship of Romain Boitard, *Design of interfaces for railway systems*, (April-June 2017)

10.2.3. Juries

10.2.3.1. Juries of PhD defences:

- Nicolas David, École Centrale Nantes, october 2017 : Nathalie Bertrand examiner;

- Thomas Geffroy, Univ. Bordeaux, december 2017: Nathalie Bertrand examiner;
- Ludovic Hofer, Univ. Bordeaux, november 2017: Blaise Genest examiner;
- Daniel Stan, École Normale Supérieure Paris-Saclay, march 2017: Nathalie Bertrand reviewer;
- Serge Tembo, Telecom Bretagne, January 2017: Éric Fabre examiner.

10.2.3.2. Other juries

- Ocan Sankur was in the computer science entrance exam jury of École Normale Supérieures and École Polytechnique.

10.3. Popularization

- Éric Badouel gave a talk at TEDx Lorient on digital democracy (coordination of citizen debates).

TOCCATA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

S. Boldo, vice-president of the 28th “Journées Francophones des Langages Applicatifs” (JFLA 2017)

S. Boldo, president of the 29th “Journées Francophones des Langages Applicatifs” (JFLA 2018)

J.-C. Filliâtre, scientific chair and co-organizer of EJCP (École Jeunes Chercheurs en Programmation du GDR GPL) at Toulouse on June 26–30, 2017. http://ejcp2017.enseeiht.fr/

10.1.1.2. Member of the Organizing Committees

S. Conchon, local chair for the 44th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2017), held in Paris, France in January 2017. http://conf.researchr.org/home/POPL-2017).

C. Marché, co-organizer of the first joint Frama-C/SPARK day (May, Paris, http://frama-c.com/FCSD17.html), in the context of the Open Source Innovation Spring (http://www.open-source-innovation-spring.org/).

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

A. Paskevich, program chair of the 9th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE 2017), in collaboration with Thomas Wies (NYU) [35].

S. Boldo, program chair of the 10th International Workshop on Numerical Software Verification (NSV 2017) in collaboration with Alessandro Abate (Oxford) [33].

S. Boldo, program vice-chair of the 28th “Journées Francophones des Langages Applicatifs” (JFLA 2017) [34].

S. Boldo, program chair of the 29th “Journées Francophones des Langages Applicatifs” (JFLA 2018).

10.1.2.2. Member of the Conference Program Committees

S. Boldo, PC of the 24th IEEE Symposium on Computer Arithmetic (ARITH 2017)

S. Boldo, PC of the 25th IEEE Symposium on Computer Arithmetic (ARITH 2018)

S. Boldo, PC of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs (CPP 2017)

S. Boldo, PC of the 7th ACM SIGPLAN Conference on Certified Programs and Proofs (CPP 2018)

S. Boldo, PC of the 8th International Conference on Interactive Theorem Proving (ITP 2017)

S. Boldo, PC of the Tenth NASA Formal Methods Symposium (NFM 2018)

G. Melquiond, PC of the 3rd International Workshop on Coq for Programming Languages (CoqPL 2017).

G. Melquiond, PC of the 1st ACM SIGPLAN Workshop on Machine Learning and Programming Languages (MAPL 2017).

G. Melquiond, PC of the 10th International Workshop on Numerical Software Verification (NSV 2017).

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, member of the editorial board of *Reliable Computing*.

S. Boldo, member of the editorial board of Binaire http://binaire.blog.lemonde.fr, the blog of the French Computer Science Society.

10.1.3.2. Reviewer - Reviewing Activities

The members of the Toccata team have reviewed numerous papers for numerous international journals.

10.1.4. Invited Talks

S. Boldo gave a talk at EDF in Palaiseau on April 20th

S. Boldo gave a talk at the ModeliScale IPL in Paris on July 4th

S. Boldo gave a talk to teachers in Luminy on May 4th

S. Boldo gave a talk at the université of Saint-Denis de la Réunion on December 8th

10.1.5. Leadership within the Scientific Community

S. Boldo, elected chair of the ARITH working group of the GDR-IM (a CNRS subgroup of computer science) with J. Detrey (Inria Nancy).

10.1.6. Scientific Expertise

C. Marché, member of the scientific commission of Inria-Saclay, in charge of selecting candidates for PhD grants, Post-doc grants, temporary leaves from universities ("délégations").

C. Marché, member of the "Bureau du Comité des Projets" of Inria-Saclay, in charge of examining proposals for creation of new Inria project-teams.

S. Boldo, member of the program committee for selecting postdocs of the maths/computer science program of the Labex mathématique Hadamard.

S. Boldo, member of a hiring committee for an associate professor position in computer science at Université Joseph Fourier, Grenoble, France.

S. Boldo, member of the 2017 committee for the Gilles Kahn PhD award of the French Computer Science Society.

10.1.7. Research Administration

G. Melquiond, member of the committee for the monitoring of PhD students (*"commission de suivi doctoral"*).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master Parisien de Recherche en Informatique (MPRI) https://wikimpri.dptinfo.ens-cachan.fr/doku.php: "Proofs of Programs" http://www.lri.fr/~marche/MPRI-2-36-1/ (M2), C. Marché (12h), A. Charguéraud (12h), Université Paris-Diderot, France.

Master: Fondements de l'informatique et ingénierie du logiciel (FIIL) https://www.lri.fr/~conchon/parcours_fiil/: "Software Model Checking" (M2), S. Conchon (9h), "Programmation C++11 avancée" (M2), G. Melquiond (16h), "Vérification déductive de programmes" (M2), A. Paskevich (10.5h), Université Paris-Sud, France.

DUT (Diplôme Universitaire de Technologie): M1101 "Introduction aux systèmes informatiques", A. Paskevich (36h), M3101 "Principes des systèmes d'exploitation", A. Paskevich (58.5h), IUT d'Orsay, Université Paris-Sud, France.

Licence: "Langages de programmation et compilation" (L3), J.-C. Filliâtre (26h), École Normale Supérieure, France.

Licence: "INF411: Les bases de l'algorithmique et de la programmation" (L3), J.-C. Filliâtre (16h), École Polytechnique, France.

Master: "INF564: Compilation" (M1), J.-C. Filliâtre (18h), École Polytechnique, France.

Licence: "Programmation fonctionnelle avancée" (L3), S. Conchon (45h), Université Paris-Sud, France.

Licence: "Introduction à la programmation fonctionnelle" (L2), S. Conchon (25h), Université Paris-Sud, France.

10.2.2. Internships

R. Rieu-Helft (ENS, Paris) was a pre-PhD student doing an internship under supervision of C. Marché and G. Melquiond. He worked on the design and the formal verification of a library for unbounded integer arithmetic [23]. He implemented in Why3 a mechanism for extracting code to the C language, in order to obtain a certified code that runs very efficiently [30].

D. Gallois-Wong was a Master-2 intern for 4 months under the supervision of S. Boldo. She began the formalization in Coq of numerical filters.

V. Tourneur was a Master-1 intern for 4 months under the supervision of S. Boldo. He developed and proved a new algorithm for computing the average of two floating-point numbers when the radix is 10.

10.2.3. Supervision

PhD in progress: M. Clochard, "Méthodes et outils pour la spécification et la preuve de propriétés difficiles de programmes séquentiels", 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 S. Conchon, F. Le Fessant et M. Mauny.

PhD in progress: F. Faissole, "Stabilité(s): liens entre l'arithmétique flottante et l'analyse numérique", since Oct. 2016, supervised by S. Boldo and A. Chapoutot.

PhD in progress: R. Rieu-Helft, "Développement et vérification de bibliothèques d'arithmétique entière en précision arbitraire", since Oct. 2017, supervised by G. Melquiond and P. Cuoq (TrustIn-Soft).

PhD in progress: D. Gallois-Wong, "Vérification formelle et filtres numériques", since Oct. 2017, supervised by S. Boldo and T. Hilaire.

10.2.4. Juries

C. Marché: reviewer of the habilitation thesis of R. Bubel, "Deductive Verification: From Theory to Practice", Technische Universität Darmstadt, Germany, November 2017.

S. Boldo: reviewer and member of the PhD defense of A. Plet, École Normale Supérieure de Lyon, Lyon, France, July 2017.

S. Boldo: reviewer and member of the PhD defense of F. Maurica, Université de la Réunion, Saint-Denis, France, December 2017.

S. Boldo: president of the PhD defense of T. Sibut-Pinote, Université Paris-Saclay, Palaiseau, France, December 2017.

10.3. Popularization

S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.

S. Boldo gave a talk at the Inria Saclay about how to popularize programming.

During the “Fête de la science” on October 13th, S. Boldo demonstrated unplugged computer science to teenagers and F. Faissole run a stand about an introduction to programming with robots. S. Boldo also did this activity to kids from 7 to 17 at the Massy opera on November, 17th.

S. Boldo gave a talk during at a *Girls can code* weekend on August 23rd in Paris.

S. Boldo went to the Arpajon high-school for presenting Women in Science on December 19th.

S. Boldo gave a popularization talk to the administrative staff of Inria at Rocquencourt for the Inria birthday on November 16th.

VERIDIS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Organization of Scientific Events

10.1.1.1. Member of the Organizing Committees

Jasmin Blanchette co-organized the *(Co)programming in Isabelle/HOL* tutorials at ICFP 2017 in Oxford, UK, and at CADE-26 in Gothenburg, Sweden.

Jasmin Blanchette co-organized the Dagstuhl Seminar on *Deduction beyond First-Order Logic* held at Schloss Dagstuhl in Germany.

Jasmin Blanchette co-organized the *(Co)programming in Isabelle/HOL* tutorials at ICFP 2017 in Oxford, UK, and at CADE-26 in Gothenburg, Sweden.

Dominique Méry was a member of the organizing committees of the workshops F-IDE [43] and IMPEX'2017.

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 2017, VTSA took place in July in Saarbrücken, Germany.

The SC^2 Summer School 2017 took place in Saarbrücken, Germany. It has been co-organized by Thomas Sturm. The school introduced graduate students and researchers from academia and industry into research and methodology in both Satisfiability Checking (SAT/SMT) and Symbolic Computation with one focus on their interconnections. It combined a thorough introduction into the theory of both fields with lectures on state-of-the-art software systems and their implementation. This was supplemented with presentations by lecturers from industry discussing the practical relevance of the topics of the school.

Together with the CADE trustees, Christoph Weidenbach started the first CADE workshop on *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2017)

10.1.2. Program Committees

10.1.2.1. Chair of Conference Program Committees

Stephan Merz co-chaired the program committee of the Fourth International Workshop on Formal Reasoning in Distributed Algorithms (FRiDA), organized in October 2017 as a satellite of DISC in Vienna, Austria.

10.1.2.2. Member of the Conference Program Committees

Jasmin Blanchette served on the program committees of the Conference on *Computer-Aided Verification* (CAV 2017), the *Conference on Automated Deduction* (CADE-26), the *International Conference on Tests and Proofs* (TAP 2017), and the Conference on *Artificial Intelligence and Theorem Proving* (AITP 2017). He also served on the following workshop committees: *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2017), *International Workshop on the Implementation of Logics* (IWIL 2017), *Proof Exchange for Theorem Proving* (PxTP 2017), and *Satisfiability Modulo Theories* (SMT 2017).

Pascal Fontaine served on the program committees of the *International Symposium on Frontiers of Combining Systems* (FroCoS 2017), the *Conference on Automated Deduction* (CADE-26) and the *International Conference on Automated Reasoning with Analytic Tableaux and Related Methods* (TABLEAUX 2017). He also served on the following workshop committees: *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2017), *Satisfiability Modulo Theories* (SMT 2017), *Satisfiability Checking and Symbolic Computation* (SC^2 2017), *Proof Exchange for Theorem Proving* (PxTP 2017)

Stephan Merz served on the program committees of the international conferences *Formal Techniques for Distributed Objects, Components, and Systems* (FORTE 2017), *Foundations of Software Technology and Theoretical Computer Science* (FSTTCS 2017), and *Formal Engineering Methods* (ICFEM 2017), the national conference *Modélisation des Systèmes Réactifs* (MSR 2017), and of the workshops FMICS-AVoCS and GRSRD.

Thomas Sturm served on the program committees of the *Second International Workshop on Satisfiability Checking and Symbolic Computation* (SC^2 2017) and the *19th International Workshop on Computer Algebra in Scientific Computing* (CASC 2017).

Uwe Waldmann served on the program committee of the workshop *International Workshop on the Implementation of Logics* (IWIL 2017) colocated with LPAR.

Christoph Weidenbach served on the program committees of the *Conference on Automated Deduction* (CADE-26) and the *International Symposium on Frontiers of Combining Systems* (FroCoS 2017). He also served on the workshop committee *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2017).

10.1.3. Journals

Jasmin Blanchette and Stephan Merz are the editors of a special issue of *Journal of Automated Reasoning* following the international conference *Interactive Theorem Proving* 2016.

Dominique Méry is the review book editor of the journal *Formal Aspects for Computing*.

Thomas Sturm is a member of the editorial boards of the *Journal of Symbolic Computation* (Elsevier) and *Mathematics in Computer Science* (Springer).

Christoph Weidenbach is a member of the editorial board of the *Journal of Automated Reasoning* (Springer).

10.1.4. Invited Talks

Jasmin Blanchette was invited to give a joint keynote talk at the FroCoS 2017, ITP 2017, and TABLEAUX 2017 conferences held in Brasília, Brazil. He presented Isabelle/HOL's support for (co)datatypes and (co)recursion [18]. He also gave invited seminar talks at the Big Proof Workshop organized by the Isaac Newton Institute in Cambridge, UK, at the TeReSe (Term Rewriting Systems) meeting in Eindhoven, the Netherlands, and at the Shonan Meeting on Automated Deduction at the Shonan Village Center in Japan.

Stephan Merz gave an invited presentation on "Formal Methods for the Cloud" at the Cloud Resiliency Workshop 2017 in Shenzhen, China.

Thomas Sturm was invited to give a keynote talk at the *3ème BIOSS Journées annuelles du groupe de travail* in Montpellier, France.

Uwe Waldmann gave an invited talk on "Saturation Theorem Proving – Basic Ideas, History, and Recent Developments" at the Seminar on Proof Assistants and Related Tools at DTU Lyngby, Denmark in October 2017.

Christoph Weidenbach gave invited talks on "Design Principles of Automated Reasoning Systems" at VSTTE 2017 and "The Role of Horn Clauses in Automatic Reasoning" at HCVS 2017.

10.1.5. Leadership within the Scientific Community

Jasmin Blanchette was elected as a regular member of the steering committee for the ITP (*Interactive Theorem Proving*) conference series, after serving for two years as an ex officio member. He is also a regular member of the CADE (*Conference on Automated Deduction*) Inc. Board of Trustees.

Pascal Fontaine is an SMT-LIB manager, together with Clark Barrett (Stanford University) and Cesare Tinelli (University of Iowa). He is a member of the FroCoS steering committee. He was an elected CADE trustee since October 2014 until October 2017 and served as a member of the Association for Automated Reasoning (AAR) board until October 2017.

Stephan Merz is a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*. He is a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS).

Thomas Sturm has been a member of the steering committee of the conference series *International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS).* His term ended in November 2017. In July 2017 he was elected as a member at large of the steering committee of the conference series *International Symposium on Symbolic and Algebraic Computation (ISSAC).*

Christoph Weidenbach is the president of CADE and a member of the steering committee of IJCAR.

10.1.6. Scientific Expertise

Pascal Fontaine was a panel member for the CASC-26 competition of first-order theorem prover. He served as an expert for the French Agence Nationale de la Recherche (ANR).

Stephan Merz served as an expert for the French Agence Nationale de la Recherche (ANR) and for the European Research Council (ERC).

Christoph Weidenbach served as an expert for the Austrian Science Fund and the University of Stellenbosch.

10.1.7. Research Administration

Dominique Méry was the head of the Doctoral School IAEM Lorraine of University of Lorraine until September 2017.

Stephan Merz is the delegate for scientific affairs at the Inria Nancy – Grand Est research center and a member of Inria’s Evaluation Committee. In 2017, he was a member of the hiring committees of junior researchers at Inria Saclay – Île de France as well as of senior researchers at Inria. He is a member of the committee for the SIF thesis award (*Prix Gilles Kahn*). He is a member of the *bureau* of the computer science committee of the doctoral school IAEM Lorraine. Until October 2017, he was a member of the Scientific Directorate of the International Computer Science Meeting Center in Schloss Dagstuhl.

Christoph Weidenbach is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master: Jasmin Blanchette, Logical Verification, 36 HETD, M1/M2, Vrije Universiteit Amsterdam, the Netherlands.

Licence: Marie Duflot-Kremer, Algorithmique et Programmation 1, 70 HETD L1 Mathématiques, Informatiques Sciences pour l’Ingénieur, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Bases de données 2, 20 HETD, L2 Informatique, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Projet personnel et communication, 60 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, 40 HETD, M2 Informatique, Université de Lorraine, France.

Master : Marie Duflot-Kremer and Stephan Merz, Conception et architectures distribuées 24 HETD M1 informatique, Université de Lorraine, France.

Licence : Pascal Fontaine, Structure des ordinateurs, 47 HETD, L2 MIASHS, parcours MIAGE, Université de Lorraine, France.

Master : Pascal Fontaine, Réseaux, 50 HETD, M1 MIAGE, Université de Lorraine, France.

Master : Pascal Fontaine, Génie Logiciel, 30 HETD, M1 MIAGE, IGA Rabbat et Université de Lorraine, Maroc.

Master: Dominique Méry, Models and algorithms, 60 HETD, M1, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Formal model engineering, 24 HETD, M2, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Modeling Systems, 30 HETD, M2, Telecom Nancy, Université de Lorraine, France.

Master: Dominique Méry, Modeling Systems, 36 HETD, M2 Informatique and Master Erasmus Mundus DESEM, Université de Lorraine, France.

Master: Dominique Méry, Event-B modeling, 8 HETD, NUI Maynooth, Ireland.

Master: Stephan Merz, Modeling and Verifying Distributed Algorithms in TLA$^+$, 8 HETD, NUI Maynooth, Ireland.

Master: Christoph Weidenbach, Automated Reasoning I & II, 150 HETD, Universität des Saarlandes, Germany.

10.2.2. Supervision

PhD: Haniel Barbosa, New techniques for instantiation and proof production in SMT solving, Université de Lorraine and UFRN (Natal, Brazil) [11]. Supervised by David Déharbe, Pascal Fontaine, and Stephan Merz, since 12/2013. Defended on September 5, 2017.

PhD: Andreas Teucke, *An Approximation and Refinement Approach to First-Order Automated Reasoning*, Saarland University. Supervised by Christoph Weidenbach, thesis submitted in October 2017.

PhD: Daniel Wand, First-Order Extensions to Support Higher-Order Reasoning, Saarland University [12]. Supervised by Christoph Weidenbach and Jasmin Blanchette, since 02/2011. Defended on August 4, 2017.

PhD in progress: Martin Bromberger, Arithmetic Reasoning, Saarland University. Supervised by Christoph Weidenbach, since July 2014.

PhD in progress: Margaux Duroeulx, SAT Techniques for Reliability Assessment, Université de Lorraine. Supervised by Nicolae Brînzei, Marie Duflot-Kremer, and Stephan Merz, since October 2016.

PhD in progress: Daniel El Ouraoui, Higher-Order SMT, Université de Lorraine. Supervised by Jasmin Blanchette, Pascal Fontaine, and Stephan Merz, since November 2017.

PhD in progress: Mathias Fleury, Formalization of Logical Calculi, Saarland University. Supervised by Christoph Weidenbach and Jasmin Blanchette, since September 2015.

PhD in progress: Souad Kherroubi, A framework to formally handle domain knowledge in system design, Université de Lorraine. Supervised by Dominique Méry, since November 2014.

PhD in progress: Nicolas Schnepf, Orchestration and Verification of Security Functions for Smart Environments, Université de Lorraine. Supervised by Rémi Badonnel, Abdelkader Lahmadi, and Stephan Merz, since October 2016.

PhD in progress: Hans-Jörg Schurr, Higher-Order SMT, Université de Lorraine. Supervised by Jasmin Blanchette, Pascal Fontaine, and Stephan Merz, since November 2017.

PhD in progress: Marco Voigt, Decidable Hierarchic Combinations, Saarland University. Supervised by Christoph Weidenbach, since November 2013.

10.2.3. Thesis committees

Stephan Merz served as a reviewer for the PhD theses of Florent Chevrou (Univ. de Toulouse), Sebastian Krings (Univ. Düsseldorf), Ognjen Marič (ETH Zurich), and Yannick Zakowski (ENS Rennes). He was an examiner for the PhD thesis of Zeinab Bakhtiarinoodeh (Univ. de Lorraine) and the habilitation of Alain Giorgetti (Univ. de Bourgogne et Franche Comté).

10.3. Science outreach

Marie Duflot-Kremer took part in various science outreach activities, with a public ranging from primary school kids to teachers and potential university students. A selection of these activities is given below.

General activities.

She is responsible for the scientific part of the fifth and last module in the Class'Code project (supervising a programming project from scratch), aiming at training teachers and educators for carrying out computer science activities with childrens aged 8 to 14 years.

Three days at "Fête de la Science" in Nancy (Faculté des Sciences et Technologies) and at Cité des Sciences, Paris, including a visit of the Minister of Higher Education and Research, Frédérique Vidal.

She is a member of the steering committee of an itinerant exhibition, intended for explaining computer science to the public, and that had its opening in early 2017.

She co-organized the SCRATCH17BDX international conference on Scratch and creative programming for kids in Bordeaux.

Activities for teachers/trainers.

She is a member of three working groups (unplugged activities, programming in secondary school and in high school) including university and secondary school teachers, dedicated to the training of math teachers. Two days of training on unplugged computer science activities were given to secondary and high school teachers.

A training session for kindergarden teachers to include in their "school project" unplugged activities related to programming for kids from 3 to 6 years old.

Several activities for the "ISN day", aimed at high school teachers teaching computer science courses.

A publication (post proceedings to appear in 2018) was accepted at the COPIRELEM colloquium, aimed at math trainers for primary school teachers.

Activities for students/pupils.

Several activities for school kids from 6 to 10 years old at Ecole Marcel Leroy, Nancy.

She was involved in the *Math en Jeans* project where secondary school kids discover what doing research means.

Various outreach activities (related to data bases, model checking, algorithms etc.) during two days aimed at presenting the university to high school students.

CARTE Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Mathieu Hoyrup is member of the Steering Committee of the Conference Series *Computability in Europe* (CiE) for the period 2017-2021.

10.1.1.2. Member of the Organizing Committees

- Mathieu Hoyrup organized the workshop Continuity, Computability, Constructivity - From Logic to Algorithms (CCC) 2017, Nancy, June 2017.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Mathieu Hoyrup was co-chair of the workshop Continuity, Computability, Constructivity - From Logic to Algorithms (CCC) 2017, Nancy, June 2017.
- Emmanuel Jeandel was PC member of STACS 2017 (https://stacs2017.thi.uni-hannover.de/) and CIE 2017 (http://math.utu.fi/cie2017/).
- Romain Péchoux is PC member of the ETAPS affiliated workshop DICE 2018 (http://cl-informatik.uibk.ac.at/users/zini/events/dice18/).
- Simon Perdrix was PC member of QPL'17 (14th International Conference on Quantum Physics and Logic, 2017, Nijmegen, the Netherlands) ; IQFA'17 (Quantum Information: Foundations and Applications, 8th IQFA's Colloquium, 2017, Nice, France). He is PC member of the forthcoming MCU'18 (8th Conference on Machines, Computations and Universality) and DCM'18 (12th International Workshop on Developments in Computational Models, FLoC 2018, Oxford, UK).
- Nazim Fatès was a member of the PC of AUTOMATA 2017.

10.1.2.2. Reviewer

- Mathieu Hoyrup reviewed articles for CiE and LICS.
- Romain Péchoux reviewed articles for ISMVL and STACS.
- Simon Perdrix reviewed articles for LICS.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Emmanuel Jeandel is member of the editorial board of RAIRO-ITA.
- Simon Perdrix is co-editor of the ERCIM issue on Quantum Computing.

10.1.3.2. Reviewer - Reviewing Activities

- Mathieu Hoyrup reviewed articles for Foundations of Computational Mathematics, Theory of Computing Systems, Mathematical Reviews.
- Romain Péchoux reviewed articles for Journal of Automated Reasoning and AMS Mathematical Reviews.
- Nazim Fatès served as a reviewer for *Natural computing* and *Theoretical computer science*.

10.1.4. Invited Talks

- Emmanuel Jeandel gave a course on Computability in Symbolic Dynamics on the Pingree Park Dynamics Workshop, http://web.cs.du.edu/~rpavlov/Pingree2017
- Emmanuel Jeandel gave a course on the Undecidability of the Domino Problem in the Winter School “Tiling Dynamical System” in Marseille, http://akiyama-arnoux.weebly.com/school.html
- Emmanuel Jeandel gave an invited talk on Higman-like theorems in symbolic dynamics at Logic Colloquium 2017, http://www.math-stockholm.se/konferenser-och-akti/logic-in-stockholm-2/logic-colloquium-201
- Romain Péchoux gave an invited talk on Higher order interpretations for higher order programs, cs department, Trinity College, Dublin.
- Simon Perdrix gave an invited talk on Measurement-based quantum computation at QPL’17 (14th International Conference on Quantum Physics and Logic, 2017).
- Simon Perdrix gave an invited talk on quantum algorithms at the event "l’Ordinateur Quantique" organised at IHP by the Fondation Sciences Mathématiques de Paris.

10.1.5. Leadership within the Scientific Community

Nazim Fatès is the vice-chair of the IFIP international working group 1.5 on Cellular automata and discrete dynamical systems.

Simon Perdrix is

- head of the GT IQ (groupe de Travail Informatique Quantique) @ GdR IM.
- board of GdR IQFA (Ingénierie Quantique, des aspects Fondamentaux aux Applications).

10.1.6. Scientific Expertise

Nazim Fatès was a project reviewer for the CONYCIT, the Chilean state agency for scientific research.

10.1.7. Research Administration

- Emmanuel Jeandel is the leader of the CARTE team.
- Isabelle Gnaedig is:
  - vice-leader of the CARTE team,
  - member of the scientific mediation committee at Inria Nancy Grand-Est.
- Emmanuel Hainry is:
  - member of the CNU (Conseil National des Universités), Section 27.
  - organizer of the CARTE Seminar.
- Simon Perdrix is Scientific Secretary at CoNRS Section 6.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence :

- Isabelle Gnaedig:
  - To the limits of the computable, 6 hours, Opening course-conference of the collegium "Lorraine INP", Nancy, France
- Emmanuel Hainry:
  - Systèmes d’exploitation, 30h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Algorithmique, 40h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Web dynamique, 60h, L1, IUT Nancy Brabois, Université de Lorraine, France

  - Bases de données, 30h, L1, IUT Nancy Brabois, Université de Lorraine, France
  - Programmation objet, 12h, L2, IUT Nancy Brabois, Université de Lorraine, France
  - Complexité, 30h, L2, IUT Nancy Brabois, Université de Lorraine, France
- Mathieu Hoyrup:
  - Bases de la Programmation Orientée Objet, 20 HETD, L2, Université de Lorraine, France
  - Interfaces Graphiques, 10 HETD, L2, Université de Lorraine, France
- Emmanuel Jeandel:
  - Algorithmics and Programming 1, 60h, L1 Maths-Info
  - Algorithmics and Programming 4, 30h, L3 Informatique
  - Modelling Using Graph Theory, 30h, L3 Informatique
  - Networking, 15h, L2 Informatique
  - Formal Languages, 30h, L3 Informatique
- Romain Péchoux:
  - Programmation orientée objet, 61,5h, L3 MIASHS
  - Programmation orientée objet, 53,5h, L2 MIASHS
  - Outils logiques pour l'informatique, 35h, L1 MIASHS
  - Bases de données, 40h, L3 Sciences de la Gestion

Master:

- Isabelle Gnaedig:
  - Design of Safe Software, Coordination of the module, M2, Telecom-Nancy (Université de Lorraine), Nancy, France,
  - Rule-based Programming, 20 hours, M2, Telecom-Nancy (Université de Lorraine), Nancy, France.
- Emmanuel Jeandel:
  - Algorithmics and Complexity, 30h, M1 Informatique
- Romain Péchoux:
  - Mathematics for computer science, 30h, M1 SCA
  - Implicit Complexity, 15h, M2 Informatique
- Simon Perdrix:
  - Pépites Algorithmiques, 6h, M1/M2 at Ecole des Mines de Nancy.
- Nazim Fatès:
  - Systèmes complexes adapatatifs, M2, 10h, Informatique (UL)
  - Agents intelligents et collectifs M1, 15h, Sciences cognitives (UL)

10.2.2. Supervision

- Emmanuel Jeandel and Simon Perdrix supervised the Master Thesis of David Zonneveld on quantum circuits.
- Nazim Fatès and Irène Marcovici supervised the Erasmus Mundus master's thesis of Jordina Francès de Mas [34].
- Emmanuel Jeandel and Simon Perdrix are advisors of Renaud Vilmart, PhD student (UL) since October 2016.

- Romain Péchoux is coadvisor of Pierre Mercuriali, PhD student, Université de Lorraine (50%, advisor: Miguel Couceiro, PR, Université de Lorraine).

10.2.3. Juries

- Emmanuel Jeandel reviewed the PhD thesis of Guilhem Gamard (Université Paul-Valery-Montpellier) and participated in the PhD defense of Laurent Grémy (Université de Lorraine), David Cattanéo (Université de Grenoble) and Sebastian Barbieri (ENS Lyon)
- Simon Perdrix participated in the PhD defense of Ruben Cohen (U. Paris Sud).

10.3. Popularization

- Nazim Fatès contributed to a booklet on the theme "Mathématiques et langages" edited by the Commission française pour l'enseignement des mathématiques (CFEM) for the forum "Mathématiques vivantes" (see http://forum-maths-vivantes.fr/-Panorama).
- This text appeared in a revised version on the CNRS website "images des mathématiques" [27].
- Nazim Fatès participated to a meeting ("projection-debat") at the Réseau et transport de l'électricité (RTE) at Villers-lès-Nancy on the these "Visages de la robotique", organised by "Sciences en lumière" (formerly Festival du film de chercheur).
- Nazim Fatès participated to a workshop on ethics in the "Forum des Sciences cognitives" organised by the "UFR mathématiques et informatique".
- Simon Perdrix gave an invited talk on quantum algorithms at the event "Mathématiques en mouvement sur l'Ordinateur quantique" organised by the Fondation Sciences Mathématiques de Paris at IHP.

CIDRE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Emmanuelle Anceaume co-chair with Maria Potop Butucaru, Christian Cachin and Shlomi Dolev the Workshop on Blockchain Technology and Theory 2017, co-located with DISC 2017.

10.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2017 (24rd Computers & Electronics Security Applications Rendez-vous), November 2017, Rennes, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) that took place in Rennes, France from 7th to 9th of June, where it gathered 600 participants.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Emmanuelle Anceaume served as a member of the following program committees:

- Algotel 2017 (19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications), May 2017, Quiberon, France.
- ICDCS 2017 (37th IEEE International Conference on Distributed Computing Systems), Atlanta, USA, 2017
- DEBS 2017 (11th ACM International Conference on Distributed and Event-based Systems), Barcelona, Spain 2017
- NCA 2017 (16th International Symposium on Network Computing and Applications), October 2017, Cambridge, MA, USA.
- PECS 2017 (3rd International Conference on Pervasive and Embedded Computing), Porto, Portugal, 2017
- ADSN2017 (6th International Workshop on Assurance in Distributed Systems and Networks, Atlanta, USA, 2017

Christophe Bidan served as a member of the following program committees:

- CRiSIS 2017 (12th International Conference on Risks and Security of Internet and Systems), September 2017, Dinard, France.
- C&ESAR 2017 (24rd Computers & Electronics Security Applications Rendez-vous), November 2017, Rennes, France.

Frédéric Majorczyck served as a member of the program committee of VizSec 2017 (IEEE Symposium on Visualization for Cyber Security), October 2017, Phoeniz, Arizona, USA.

Guillaume Piolle served as a member of the program committee of APVP 2017 (Atelier sur la Protection de la Vie Privée), June 2017, Autrans, France.

Eric Totel served as a member of the program committee of RESSI 2017 (Les Rendez-vous de la recherche et de l'enseignement en sécurité des systèmes d'information).

Frédéric Tronel served as a member of the program committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) June 2017, Rennes, France.

Gilles guette served as a member of the following program committees:

- ICISSP 2017 (International Conference on Information System Security and Privacy), February 2017, Porto, Portugal.

10.1.2.2. Reviewer

- Gilles Guette - IEEE ISNCC 2017 (IEEE International Symposium on Networks, Computers and Communications).
- Michel Hurfin - NCA 2017 (16th International Symposium on Network Computing and Applications).
- Jean-François Lalande - ICISSP 2017 (3rd International Conference on Information Systems Security and Privacy).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Michel Hurfin belongs to the editorial board of the Springer open access journal of Internet Services and Applications.

10.1.3.2. Reviewer - Reviewing Activities

- Emmanuelle Anceaume - Elsevier JPDC (Journal of Parallel and Distributed Computing), Performance Evaluation, IEEE TDSC (Transactions on Dependable and Secure Computing), and IEEE TPDS (Transactions on Parallel and Distributed Systems).
- Michel Hurfin - Springer JISA (Journal of Internet Services and Applications) and Springer TOCS (Theory of Computing Systems).
- Jean-François Lalande - IARIA IJAS (International Journal on Advances in Security), and Elsevier Computer Communications (International Journal for the Computer and Telecommunications Industry).
- Guillaume Piolle - ACM TOIT (Transactions on Internet Technologies).
- Eric Totel - IEEE Transactions on Reliability.

10.1.4. Invited Talks

Emmanuelle Anceaume was invited to give

- a keynote at Algotel 2017, May 2017, entitled "Bitcoin and its distributed ledger"
- a keynote at WIFS 2017, December 2017, entitled: "A primer on blockchain technology and the bitcoin cryptocurrency"

10.1.5. Leadership within the Scientific Community

Ludovic Mé serves the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).

Ludovic Mé chairs the steering Committee of the annual French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information). He is a member of the Steering Committee of the annual international conference RAID (International Symposium on Research in Attacks, Intrusions and Defenses).

10.1.6. Research Administration

Emmanuelle Anceaume has participated in various juries (Post-doctoral grants, delegation Inria, PEDR Inria). As a member of the CE Inria, Emmanuelle Anceaume has participated to the hiring committee CR2/CR1 of Rennes and Sophia Antipolis.

Michel Hurfin is the local representative of the "mission jeunes chercheurs" in Rennes. He is a member of the "Commission personnel" and is in charge of the PhD student recruitment campaign of Inria Rennes Bretagne Atlantique. He is a member of the councils of the doctoral school Matisse. He is a member of the advisory board of the doctoral training center of EIT Digital in Rennes.

Ludovic Mé acts as Scientific Officer for the Rennes - Bretagne Atlantic Inria Research Center. As such, he is also a member of the Evaluation Commission and of the Internal Scientific Council of Inria.

Ludovic Mé leads the expert group dedicated to the evaluation of the French laboratories working in the "computing and telecom" domain, relatively to the way they protect their scientific and technical patrimony (PPST French regulation).

Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR). Valérie Viet Triem Tong has also participated in the Inria post-doctoral grant.

10.2. Teaching - Supervision - Juries

10.2.1. Certification

The master degree program "Mastère Spécialisé en Cybersécurité" has received the SecNum*edu* label. This label testifies that this program meets the requirements of a charter that has been jointly established by ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) and various actors (administrations, companies, ...) of the domain. This label was awarded during the annual Forum International de la Cybersécurité (FIC) in January 2017 at Lille.

10.2.2. Teaching

- Master: Emmanuelle Anceaume, *Research in Computer Science - Distributed Algorithms*, 20 hours of lecture, M2; Université Rennes 1, France;
- Licence: Christophe Bidan, *Algorithms and Data Structures*, 36 hours of lecture including 7.5 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;
- Licence: Christophe Bidan, *Software Engineering*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence: Christophe Bidan, *Supervision of student project*, 1 project, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan is responsible for the module *Secured information systems*, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan, *Applied cryptography*, 6 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;
- Master: Christophe Bidan, *Applied cryptography*, 15 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master : Christophe Bidan, *Cryptographic Protocols*, 6 hours of lecture, mastère CS (Cyber Security), CentraleSupélec, France;
- Master: Christophe Bidan, *Information systems*, 4.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan, *Supervision of student project*, 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Licence: Gilles Guette, *Algorith and Complexity*, 28 hours, L1 - Licence, ISTIC/University of Rennes, France;
- Licence: Gilles Guette, *Network Initiation*, 57.5 hours, L3 - Licence, ISTIC/University of Rennes, France;

- Licence: Gilles Guette, *Network Initiation*, 41.5 hours, L3 - first year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Routing*, 32 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Mobile Network Routing*, 5 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Advanced Network Services*, 10 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Project*, 24 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Security*, 28 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network and System Security*, 12 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Modeling*, 18 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Sensors Network*, 30 hours, M2 - Master, ISTIC/University of Rennes, France;
- Master: Gilles Guette, *Supervision of student*, Contrat de professionnalisation, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Supervision of student internship*, M2 - ISTIC/University of Rennes, France;
- Licence: Guillaume Hiet, *Algorithms and Data Structures*, 12.5 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Computer security and privacy for the engineer*, 8 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master: Guillaume Hiet, *Pentest*, 19 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Pentest*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master: Guillaume Hiet, *Introduction to Linux*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master: Guillaume Hiet, *Java Security*, 4.5 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;
- Master: Guillaume Hiet, *Linux Security*, 18 hours, M2 - Mastère Spécialisé CS , CentraleSupélec, France;
- Master: Guillaume Hiet, *Linux Security*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *LDAP*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 15 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 13.5 hours, M2 - third year of the engineer degree, M2 research degree of University of Rennes 1, CentraleSupélec, France;

- Master: Guillaume Hiet, *Security Monitoring*, 3 hours, M2, cycle "Sécurité Numérique", INHESJ, France;
- Master: Guillaume Hiet, *Computer Security*, 31.5 hours, M2, Mastère Spécialisé Architecte des Systèmes d'Information, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 16 hours, M2, University of Rennes 1, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 10 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 9 hours, M2, Université of Limoges, France;
- Master: Guillaume Hiet, *Firewall*, 6 hours, M2, University of Rennes 1, France;
- Master: Guillaume Hiet, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master:Jean-François Lalande, *Legal aspects of information security*, 3.5 hours, M2 - master CyberSecurity, CentraleSupélec, France;
- Master: Guillaume Hiet, *Android Malware*, 3.5 hours, M2, Mastère Spécialisé CS (Cyber Security), France;
- Master: Jean-François Lalande, *Supervision of student project*, 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Jean-François Lalande, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Jean-François Lalande, *Supervision of student project*, 1 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering*, 18 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering tutorials*, 6 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering and Java development*, 18 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master : Ludovic Mé, *Information systems tutorials*, 6 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Ludovic Mé, *Supervision of student project*, 1 project, 38 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Licence: Guillaume Piolle, *Software engineering*, 1.5 hours, L3 - first year of the engineering degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Modelling, Algorithms and Programming*, 22 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computer security and privacy*, 5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Software project*, 3.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Relational databases*, 6 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

- Master: Guillaume Piolle, *Computer networks*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Security Policies*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Java programming*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computer networks*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Software engineering*, 12 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Network Access Control*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Web development*, 32 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Privacy protection*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computing project*, 60 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Legal aspects of information security*, 4.5 hours, M2 - master CyberSecurity, CentraleSupélec, France;
- Licence : Eric Totel, *Foundations of computer science, data structures and algorithms*, 9 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Eric Totel, *Software Modeling*, 15 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Operating Systems*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *C language*, 24 hours including 6 hours of lecture, M2 - master CS (Cyber Security), CentraleSupélec, France;
- Master : Eric Totel, *C language and C++ language*, 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Dependability* , 9 hours including 7.5 hours of lecture, M2 - third year of the engineer degree and master research, CentraleSupélec, France;
- Master : Eric Totel, *Dependability*, 3 hours of lecture, M2 - third year of the engineer degree (ingénierie des systèmes automatisés), CentraleSupelec, France;
- Master : Eric Totel, *Dependability*, 4.5 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), CentraleSupélec, France;
- Master : Eric Totel, *Intrusion Detection*, 6 hours of lecture, M2 - M2 - master CS (Cyber Security), CentraleSupélec, France;
- Master : Eric Totel, *Intrusion Detection*, 9 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;
- Master : Eric Totel, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Supervision of student project,* 1 project, M2 - third year of the engineer degree, CentraleSupélec, France;
- Licence: Frédéric Tronel, *Software engineering*, 40 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

- Licence: Frédéric Tronel, *Operating Systems*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel is responsible of the M2 degree in *CyberSecurity* (mastère spécialisé), organized jointly by CentraleSupélec and Institut Mines Télécom (IMT) Atlantique, France;
- Master: Frédéric Tronel, *Operating systems*, 21 hours hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Compilers*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Automatic reasoning*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Assembly Language*, 6 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 20.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Firewall*, 15 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Calculability in distributed systems*, 6 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;
- Master: Frédéric Tronel, *Computer network*, 8 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;
- Licence : Valérie Viet Triem Tong, *Algorithms and Data Structures*, 36 hours of lecture including 7 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;
- Licence : Valérie Viet Triem Tong, *Supervision of student project*, 6 projects of 2nd year of the engineer degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Games Theory*, 18 hours, M1 - second year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Formal Methods*, 9 hours, M2 - third year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Intrusion detection using information flow control*, 9 hours, M2 / third year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Programming in Java*, 12 hours, M1 - international students (NplusI) second year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Small elements of decidability*, 7.5 hours, M2 - third year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Supervision of student project*, 1 project, mastere CS (Cyber Security), CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Supervision of student project*, 8 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Supervision of student project*, 1 project year of the engineer degre, CentraleSupélec, France;
- Doctorant : Valérie Viet Triem Tong, *Malware analysis by OS information flow tracking*, 2 hours, Summerschool - Cyber in Berry, Bourges, France;

10.2.3. Supervision

10.2.3.1. Theses defended in 2017

- PhD: Laurent Georget, *Suivi de flux d'information correct pour les systèmes d'exploitation Linux*, Octobre 2017, supervised by Mathieu Jaume (25% - MdC LIP6), Guillaume Piolle (25%), Frédéric Tronel (25%), and Valérie Viet Triem Tong (25%);
- PhD: Deepak Subramanian, *Multi-level Information Flow Monitoring*, started in January 2013, supervised by Christophe Bidan (20%) and Guillaume Hiet (80%);
- PhD: Antoine Guellier, *Utilisation de la cryptographie homomorphe pour garantir le respect de la vie privée*, started in October 2013, supervised by Christophe Bidan (50%) and Nicolas Prigent (50%);
- PhD: Kun He, *Mise en œuvre de techniques de droit à l'oubli pour les contenus numériques*, started in October 2013, supervised by Christophe Bidan (50%) and Gaetan LeGuelvouit (50% - IRT B-Com);
- PhD: Solenn Brunet, *Privacy-preserving location-based services*, started in October 2014, supervised by Christophe Bidan(40%), Sébastien Gambs (30%) and Jacques Traoré (30% - Orange Labs Caen);
- PhD: Florian Grandhomme, *Protocole de routage externe type BGP dans un environnement réseaux tactiques adhoc mobiles : faisabilité et performances*, started in October 2014, supervised by Gilles Guette (50%), Adlen Ksentini (25% - Eurecom), and Thierry Plesse (25% - DGA MI).

10.2.3.2. Theses in progress

- PhD in progress: Mouna Hkimi, *Détection d'intrusion dans les systèmes distribués*, started in October 2013, supervised by Eric Totel (50%) and Michel Hurfin (50%);
- PhD in progress: Thomas Letan, *Contribution à la sécurité des couches basses des systèmes d'information*, started in January 2015, supervised by Guillaume Hiet (50%), Pierre Chifflier (25% - ANSSI), and Ludovic Mé (25%);
- PhD in progress: Damien Crémilleux, *Visualisation d'évènements de sécurité pour la supervision*, started in October 2015, supervised by Christophe Bidan (30%), Nicolas Prigent (35%), and Frédéric Majorczyk (35% - DGA MI);
- PhD in progress: Mourad Leslous, *Déclenchement automatique de codes jugés suspects dans les applications Android*, started in October 2015, supervised by Thomas Genet (20% - Celtique Inria project), Jean François Lalande (40% - INSA Centre Val de Loire), and Valérie Viet Triem Tong (40%);
- PhD in progress: Mounir Nasr Allah, *Contrôle de flux d'information par utilisation conjointe d'analyse statique et d'analyse dynamique accélérée matériellement*, started in November 2015, supervised by Guillaume Hiet (75%) and Ludovic Mé (25%);
- PhD in progress: Pernelle Mensah, *Adaptation de la Politique de Sécurité guidée par l'Évaluation du Risque dans les Infrastructures de Communication modernes*, started in January 2016, supervised by Eric Totel (25%), Guillaume Piolle (25%), Christine Morin (25% - Myriad Inria project), and Samuel Dubus (25% - Nokia);
- PhD in progress: David Lanoë, *Détection d'intrusion dans les applications distribuées : l'approche comportementale comme alternative à la corrélation d'alertes*, started in october 2016, supervised by Michel Hurfin (50%) and Eric Totel (50%);
- PhD in progress: Aurélien Trulla, *Caractérisation de malware Android par suivi de flux d'information et nouvelles techniques d'évasion*, started in October 2016, supervised by Jean Louis Lanet (25% - Tamis Inria project) and Valérie Viet Triem Tong (75%);
- PhD in progress : Ronny Chevalier , "Enhanced computer platform security through an intrusion-detection approach", started in November 2016, supervised by Guillaume Hiet (50%), Boris Balacheff (25% - HP), and Ludovic Mé (25%);
- PhD in progress: Laetitia Leichtnam, *Visualisation pour la caractérisation d'événements de sécurité*, started in october 2016, supervised by Eric Totel (40%), Nicolas Prigent (30%) and Ludovic Mé (30%);

- PhD in progress : Charles Xosanavongsa, *Combining Attack Specification and Dynamic Learning from traces for correlation rule generation*, started in december 2016, supervised by Eric Totel (50%) and Ludovic Mé (50%);
- PhD in progress : Pierre Graux, *Security of Hybrid Mobile Applications*, started in october 2017, supervised by Valérie Viet Triem Tong (50%) and Jean-Francçois Lalande (50%);
- PhD in progress : Vasile Cazacu, *Calcul distribué pour la fouille de données cliniques*, started February 2017, supervised by Emmanuelle Anceaume (50%) and Marc Cuggia (50%)
- PhD in progress : Aurélien Dupin, *Secure multi-partie computations*, started February 2016, supervised by Christophe Bidan(40%), David Pointchavalm (30% - ENS) and Renaud Dubois (30% - Thales).

10.2.3.3. Supervision of external PhD candidates

- LL. D. (Doctor of Laws) in progress: Gustav Malis, *Droit à l'effacement des données mises à disposition par les personnes elles-mêmes*, started in March 2014, supervised by Annie Blandin (80% - IODE) and Guillaume Piolle (20%);
- PhD in progress: Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, started in January 2015, supervised by Stéphane Mocanu (50% - Gipsa-lab), Guillaume Hiet (25%), and Jean-Marc Thiriet (25% - Gipsa-lab);
- PhD in progress : Yves Mocquard, *Population protocols*, started in september 2015, supervised by Bruno Sericola (Dyonisos Inria project) and Emmanuelle Anceaume;.

10.2.4. Juries

Ludovic Mé was a member of the PhD committee for the following PhD and HDR thesis:

- Pierre Laperdrix, *Browser Fingerprinting: Diversity to Augment Authentication and Build Client-side Countermesures*, INSA of Rennes, 03/10/2017 (President of the Jury);

Ludovic Mé has reported the following PhD thesis:

- Pierre Parrend, *Emergent Industrial Ecosystems*, University of Strasbourg, 12/12/2017.

Christophe Bidan was a member of the PhD committee for the following PhD thesis:

- Jean Aimé Maxa, *Architecture de communication sécurisée d'une flotte de drones*, Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier), 28/06/2017;
- Eric Asselin, *Système de détection d'intrusion adapté au système de communication aéronautique ACARS*, Institut National Polytechnique de Toulouse (INP Toulouse), 28/06/2017 (reviewer);

Jean-François Lalande has reported the following PhD thesis:

- Julien Hatin, *Evaluation de la confiance dans un processus d'authentification*, 24/11/2017.

Eric Totel was a member of the PhD commitee for the following PhD thesis:

- Giannakou Anna, *Self-Adaptable Security Monitoring for IaaS Cloud Environments*, 06/07/2017 (President of the Jury).
- Yacine Hebbal, *Semantic monitoring mechanisms dedicated to security monitoring in IaaS cloud*, 18/09/2017 (President of the Jury).

Valérie Viet Triem Tong has reported the following PhD thesis:

- Franck de Goer de Herve, *Rétro-ingénierie de programmes binaires en une exécution - une analyse dynamique légère basée au niveau des fonctions*, 10/20/2017.

10.3. Popularization

Valérie Viet Triem Tong has participated to the scientific television show *l'Esprit Sorcier* recorded at *Musée des Sciences et de l'Industrie* during the *Fête de la Science*. She has also participated to the scientific promotion movie about *High Security Laboratory* recorded at Nancy.

Damien Crémilleux has participated to the event "Ma thèse en 180s" and the "RCC challenge: my thesis 3.0" for the popularization of his work's thesis on security visualization.

COMETE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing committee

Catuscia Palamidessi is member of:

The Executive Committee of SIGLOG, the ACM Special Interest Group on Logic and Computation. Since 2014.

The Organizing Committee of LICS, the ACM/IEEE Symposium on Logic in Computer Science. Since 2010.

The Steering Committee of ETAPS, the European Joint Conferences on Theory and Practice of Software. Since 2006.

The Steering Committee of EACSL, the European Association for Computer Science Logics. Since 2015.

The Steering Committee of CONCUR, the International Conference in Concurrency Theory. Since 2016.

The Steering Committee of FORTE, the International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Since 2014.

The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007.

The IFIP Working Group 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

The IFIP Working Group 1.8 – Concurrency Theory.

Frank D. Valencia is member of:

The steering committee of the International Workshop in Concurrency EXPRESS. Since 2010.

8.1.2. Scientific events selection

8.1.2.1. Member of conference program committees

Catuscia Palamidessi is/has been a member of the program committees of the following conferences and workshops:

PETS 2019. The 19th Privacy Enhancing Technologies Symposium. July 2019.

TASE 2018. The 12th International Symposium on Theoretical Aspects of Software Engineering Guangzhou, China, 29-31 August 2018.

PETS 2018. The 18th Privacy Enhancing Technologies Symposium. Barcelona, Spain, 24-27 July 2018.

FOSSACS 2018. The 21st International Conference on Foundations of Software Science and Computation Structures. (Part of ETAPS 2018.) Thessaloniki, Greece, 14-21 April 2018.

SOFSEM 2018. The 44th Annual Int'l Conference on Current Trends in Theory and Practice of Computer Science (track on Foundations of Computer Science). Krems an der Donau, Austria, 29 January- 2 February, 2018.

ICTAC 2017. The 14th International Colloquium on Theoretical Aspects of Computing. Hanoi, Vietnam, 23-27 October 2017.

TASE 2017. The 11th International Symposium on Theoretical Aspects of Software Engineering. Nice, France, 13-15 September 2017.

CONCUR 2017. The 28th International Conference on Concurrency Theory. Berlin, Germany, 5-8 September 2017.

CSL 2017. The 26th EACSL Annual Conference on Computer Science Logic. Stockholm, Sweden, 20-25 August 2017.

ICSOFT-PT 2017. The 12th International Conference on Software Paradigm Trends. Lisbon, Portugal, 24-26 July 2017.

ICALP 2017 (Track B). The 44th International Colloquium on Automata, Languages, and Programming. Warsaw, Poland, 10–14 July 2017.

FORTE 2017. The 37th IFIP International Conference on Formal Techniques for Distributed Objects, Components, and Systems. Neuchâtel, Switzerland, 19-22 June 2017.

CSR 2017. The 12th International Computer Science Symposium in Russia. Kazan, Russia, 8–12 June 2017.

Konstantinos Chatzikokolakis is/has been a member of the program committees of the following conferences and workshops:

BMDA 2018: Workshop on Big Mobility Data Analytics

QAPL 2018: International Workshop on Quantitative Aspects of Programming Languages and Systems

HotSpot 2018: 6th Workshop on Hot Issues in Security Principles and Trust

ICDE 2017: IEEE International Conference on Data Engineering

CSF 2017: 30th IEEE Computer Security Foundations Symposium

POST 2017: 6th International Conference on Principles of Security and Trust

BIGQP 2017: International Workshop on Big Geo Data Quality and Privacy

Frank D. Valencia is/has been a member of the program committees of the following conferences and workshops:

RADICAL-2017. International Workshop Recent Advances in Concurrency and Logic - RADICAL

CP-ICLP-SAT-DP-17. Doctoral Program of the 23rd International Conference on Principles and Practice of Constraint Programming

8.1.2.2. Reviewing

The members of the team reviewed several papers for international conferences and workshops.

8.1.3. Journals

8.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

Member of the Editorial Board of Proceedings on Privacy Enhancing Technologies (PoPETs), published by De Gruyter.

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press.

Member of the Editorial Board of Acta Informatica, published by Springer.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, published by Elsevier Science.

Member of the Editorial Board of LIPIcs: Leibniz International Proceedings in Informatics, Schloss Dagstuhl–Leibniz Center for Informatics.

Konstantinos Chatzikokolakis is:

Editorial board member of the newly established Proceedings on Privacy Enhancing Technologies (PoPETs), a scholarly journal for timely research papers on privacy.

8.1.3.2. Reviewing

The members of the team regularly review papers for international journals and conferences.

8.1.4. Other Editorial Activities

Frank D. Valencia has been:

Co-editor of the special issue on Mathematical Structures in Computer Science dedicated to the best papers from the 12th International Colloquium on Theoretical Aspects of Computing.

8.1.5. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

Member of the committee for the assignment of the Inria International Chairs.

Member of the committee for the Alonzo Church Award for Outstanding Contributions to Logic and Computation. Since 2015. In 2018 Palamidessi is the president of this committee.

President of the selection committee for the EATCS Best Paper Award at the ETAPS conferences. Since 2006.

8.1.6. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

FACS 2017. The 14th International Conference on Formal Aspects of Component Software. Barga, Portugal. 10-13 Oct, 2017.

Cybersecurity 2017. Focus Day on Cyber Security and Helthcare. In the context of the European Cyber Week. Rennes, France, 30 November 2017.

QuaSy 2017. Quantitative Systems: Theory and Applications. Como, Italy, 16-17 October 2017.

Women in Logic 2017, Reykjavik, Island, June 2017.

CrossFyre 2017 Workshop on Cryptography, Robustness, and Provably Secure Schemes. Paris. April 2017.

FORSE 2017 (Keynote speaker). 1st International Workshop on FORmal methods for Security Engineering. Porto, Portugal. 19–21 February, 2017.

8.1.7. Service

Catuscia Palamidessi has served as:

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). May 2016 - .

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Frank D. Valencia has been teaching the undergraduate course "Computability", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. July 27 - Nov 1, 2017.

Master : Frank D. Valencia has been teaching the masters course "Foundations of Computer Science", 45 hours, at the Pontificia Universidad Javeriana de Cali, Colombia. Jan 27 - Jun 1, 2017.

Master: Konstantinos Chatzikokolakis and Catuscia Palamidessi have been teaching a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. 2016-17 and 2017-18. Total for each semester: 24 hours plus 6 hours for the exam and the exercise session is preparation to the exam.

8.2.2. Supervision

PhD in progress (2017-) Marco Romanelli. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Moreno Falaschi (University of Siena, Italy). Thesis subject: Application of Information Flow to feature selection in machine learning.

PhD in progress (2017-) Anna Pazii. Co-supervised by Konstantinos Chatzikokolakis and Catuscia Palamidessi. Thesis subject: Local Differential Privacy.

PhD in progress (2016-) Tymofii Prokopenko. Ecole Polytechnique and ENS Cachan. Grant Digiteo-Digicosme. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Serge Haddad (ENS Cachan).

PhD in progress (2017-) Sergio Ramirez. Co-supervised by Frank Valencia and Camilo Rueda, Universidad Javeriana Cali. Thesis subject: Quantitive Spatial Constraint Systems.

PhD terminated (2015-17) Joris Lamare. Ecole Polytechnique. Grant MSR Center. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis. Joris has stopped his PhD due to personal reasons.

PhD completed (2014-17) Michel Guzman. Titile: On the Expressiveness of Spatial Constraint Systems [11]. Ecole Polytechnique. Grant Inria CORDI-S. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

8.2.3. Juries

Catuscia Palamidessi has been reviewer and member of the board at the PhD defense for the thesis of the following PhD student:

Nicolas Bonifas (Ecole Polytechnique, France). Member of the committee board at the PhD defense. Title of the thesis: *Geometric and Dual Approaches to Cumulative Scheduling*. Supervised by Philippe Baptiste. Defended in December 2017.

Maggie Mhanna (CentraleSupelec, France). Member of the committee board at the PhD defense. Supervised by Pablo Piantanida. Defended in January 2017.

8.2.4. Other didactical duties

Catuscia Palamidessi is:

Member of the advising committee for Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden, since 2014. Also reviewer and member of the committee for the halfway thesis defense (Licentiate) that took place in June 2015.

External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.

Member of the advising committee for the PhD of Jun Wang (PhD student supervised by Qiang Tang and Peter Ryan), University of Luxembourg. Since December 2014.

Member of the advising committee for the PhD of Andrea Margheri (PhD student supervised by Rosario Pugliese), University of Florence, Italy. 2014-16.

Konstantinos Chatzikokolakis and Catuscia Palamidessi have designed, and coordinate, a course on the Foundations of Privacy at the MPRI, the Master Parisien pour la Recherche en Informatique. University of Paris VII. A.Y. Since 2015.

DATASPHERE Team

9. Dissemination

9.1. Promoting Scientific Activities

Stéphane Grumbach has been co-director of IXXI since 2014. He is also involved in the Anthropocene Group at ENS Lyon, which promoted interdisciplinary research and teaching activities on issues related to the adaptation to the changes of the natural ecosystem. He is involved in various initiatives to promote scientific knowledge to a wider audience, as well as in cooperation with public administrations (local and national) to face the challenges of the digital revolution.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Stéphane Grumbach teaches a new Master course on the Economy of Data at SciPo Paris. He also teaches in several universities including, ENS Lyon, Insa Lyon, etc.

9.2.2. Supervision

PhD : Robert Riemann, Towards Trustworthy Online Voting: Distributed Aggregation of Confidential Data, Université de Lyon, 18 décembre 2017, directeur de thèse Stéphane Grumbach

PhD in progress : Jingxiu Su, DNS data analysis, 2016, directeur de thèse Kave Salamatian

PESTO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

V. Cortier was auditioned by the chamber of the workers in Luxembourg, on the security of electronic voting.

10.1.1. Scientific Events Selection

10.1.1.1. Program Committee Chair

- A. Imine: FPS 2017, 10th International Symposium on Foundations & Practice of Security, Nancy, October 23-25, 2017 (co-chair with J. M. Fernandez, Polytechnique Montreal, Canada)
- M. Rusinowitch: SCSS 2017, The 8th International Symposium on Symbolic Computation in Software Science, Gammarth, Tunisie, April 6-9, 2017 (co-chair with M. Mosbah, Univ Bordeaux)

10.1.1.2. Program Committee Member

- V. Cortier: E-VoteID 2018, POST 2018, E-VoteID 2017, CCS 2017, LICS 2017, SAC 2017, HotSpot 2017
- S. Kremer: Voting 2018, EuroS&P 2018, PLAS 2017, ESORICS 2017, Voting 2017, EuroS&P 2017
- C. Ringeissen: IJCAR 2018, UNIF 2018, WRLA 2018, FroCoS 2017, UNIF 2017
- M. Rusinowitch: CRISIS 2017, FPS 2017, ICISSP 2018, IWSPA 2018
- V. Cheval: TMPA 2017, SEC@SAC 2017

10.1.2. Journal

10.1.2.1. Editorial Board Member

- V. Cortier: Information & Computation, Journal of Computer Security, ACM Transactions on Privacy and Security (TOPS, previously TISSEC), Foundations and Trends (FnT) in Security and Privacy
- S. Kremer: ERCIM News

10.1.2.2. Scientific Committee Member

- L. Vigneron: Technique et Sciences Informatiques, Lavoisier

10.1.3. Invited Talks

- V. Cortier. Invited tutorial at Highlights 2017, London, UK, September 12th, 2017
- V. Cortier. Invited talk at FPS 2017, Nancy, France, October 2017
- V. Cortier. Invited talk at CIAA 2017, Marne-la-Vallée, France, June 2017
- V. Cortier. Invited talk at Workshop on the 20th Anniversary of LSV, Cachan, France, May 11th 2017
- V. Cortier. Invited tutorial at ETAPS 2017, Uppsala, Sweden, April 22nd, 2017
- V. Cortier. Invited talk at Models and Tools for Security Analysis and Proofs Workshop, affiliated with Eurocrypt 2017, Paris, France, April 29th 2017

10.1.4. Research Administration

Inria evaluation committee (S. Kremer)

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (S. Kremer)

Jury Junior Research Position Inria Nancy-Grand Est (V. Cortier, committee chair)

Jury Professor at UMPC, LIP6 (V. Cortier)

Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

  V. Cheval, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 69 hours (ETD), TELECOM Nancy

  J. Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 146 hours (ETD), TELECOM Nancy
- Master:

  V. Cortier, Security of flows, 20 hours, M2 Computer Science, TELECOM Nancy and Mines Nancy

  A. Imine, Security for XML Documents, 12 hours (ETD), M1, Univ Lorraine

  S. Kremer, Security Theory, 24 hours (ETD), M2 Computer science, Univ Lorraine

  C. Ringeissen, Decision Procedures for Software Verification, 18 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 22.5 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 24 hours (ETD), M2 MIAGE – Distributed Information Systems, Univ Lorraine

  L. Vigneron, Security of information systems, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine
- Summer School:

  V. Cortier and S. Kremer: Summer School on Models and Tools for Cryptographic Proofs, Nancy, June 2017

10.2.2. Supervision

- PhD in progress:

  Younes Abid, Privacy control for social networks, started in March 2015 (M. Rusinowitch)

  Antoine Dallon, Decision procedures for equivalence properties, started in November 2015 (V. Cortier and S. Delaune)

  Alicia Filipiak, Design and validation of security services for mobile platforms: smartphones and tablets, started in March 2015 (V. Cortier)

  Abreha Haftay Gebreslasie, Compressed and Verifiable Filtering Rules in Software-defined Networking, started in September 2017 (A. Lahmadi, M. Rusinowitch and A. Bouhoula)

  Charlie Jacomme, Security protocols: new properties, new attackers, new protocols, started in September 2017 (H. Comon and S. Kremer)

  Joseph Lallemand, Type systems for equivalence properties, started in September 2016 (V. Cortier)

  Itsaka Rakotonirina, Efficient verification of equivalence properties in cryptographic protocols, started in October 2017 (V. Cheval and S. Kremer)

  Ludovic Robin, Verification of cryptographic protocols using weak secrets, started in October 2014, defense scheduled early 2018 (S. Delaune and S. Kremer)

10.2.3. Juries

Examiner for Robin David, CEA and Loria (S. Kremer)

Reviewer for Ryan Stanley-Oakes, Univ Bristol (S. Kremer)

Examiner and president of the jury for Wazen Shbair, Univ Lorraine, Loria (V. Cortier)

Examiner and president of the jury for Hubert Godefroy, Univ Lorraine, Loria (V. Cortier)

Reviewer for Fabienne Eigner, Univ Saarbruecken (V. Cortier)

Reviewer for Mnacho Echenim, HDR, Univ Grenoble (M. Rusinowitch)

10.3. Popularization

- How to Explain Modern Security Concepts to your Children [11] (J. Dreier)
- Vote par Internet [41] (V. Cortier and S. Kremer)
- 2 days of debate on privacy at *Moments d'invention 2016*, organized by Grand Nancy (V. Cortier)
- booth at the *Open Government Summit* organized at Sénat (V. Cortier)
- Conference and debate at the *ISN day*, conference for teachers in computer science (V. Cortier)
- Interview for *silicon.fr* on weakening cryptosystems to allow limited access by authorities (S. Kremer)
- France 3 Lorraine radio interview on computer security (S. Kremer)
- Interview for *AFP* on electronic voting (S. Kremer)
- Interview for *AFP* and *Huffington Post* on electronic voting (V. Cortier)

PRIVATICS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

C. Castelluccia: Co-chair of the DTL Grant program (http://datatransparencylab.org/grants-program/), Co-chair of the Workshop on "Intelligence Oversight", (Nov., Montbonnot).

D. Le Metayer: APVP 2017 (Jun., Autrans), panel on "Algorithms: too intelligent to be intelligeable ?" at CPDP 2017 (Jan., Brussels).

M. Cunche: APVP 2017 (Jun., Autrans).

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

C. Castelluccia: DTL Grant program, ACM Symposium on Applied Computing (Privacy by Design in Practice track).

D. Le Métayer: CSF 2017, IWPE 2017, APF 2017, CPDP 2017, Conference "Converging trends between law and digital technologies".

V. Roca: VTC 2017, SPACOMM 2017, SpaCCS 2017.

M. Cunche: Mobiquitous 2017, ICISSP 2017.

9.1.3. Invited Talks

D. Le Métayer on *Intelligence and the scientific community*, organized by the French Intelligence Academy in partnership with the Academy of Technologies, (Paris, Jun. 2017).

D. Le Métayer on *Personal data protection*, organized by ANVIE (Association nationale de valorisation interdisciplinaire de la recherche en sciences humaines et sociales auprès des entreprises), (Paris, May 2017).

D. Le Métayer on *The ethics of algorithms*, organized by FFA (Fédération Française des Assurance), (Paris, Jul. 2017).

D. Le Métayer on *Algorithmes prédictifs: Quels enjeux éthiques et juridiques?*, organized by CREOGN (Centre de recherche de l'École des officiers de la gendarmerie nationale), (Paris, Oct. 2017).

D. Le Métayer on *Capacity: an abstract model of control over personal data* invited talk at Chalmers University, (Göteborg, Nov. 2017).

Claude Castelluccia on *Promoting Peace on the Internet*, organized by Unesco (Paris, Apr. 2017).

Claude Castelluccia Oxford Internet Institute, (Oxford, Jul. 2017).

9.1.4. Leadership within the Scientific Community

C. Castelluccia: member of the scientific committee of the CNIL-Inria Privacy Award, co-creator and board member of the Amnesys (Alpine Multidisciplinary NEtwork on CYber-security Studies) group (http://amnecys.inria.fr), co-leader of the WP5 of the Data Institute of UGA (https://data-institute.univ-grenoble-alpes.fr).

D. Le Métayer: member of the scientific committee of the CNIL-Inria Privacy Award, member of the editorial committee of the Transalgo Inria platform.

V. Roca: co-chair of the research group NWCRG (Network Coding Research Group) of IRTF (Internet Research Task Force).

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 : Mathieu Cunche, *Introduction to computer science*, 120h, L1, INSA-Lyon, France.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.

Undergraduate course : Mathieu Cunche, *Advanced Topics in Security*, 20h, L3, ENSIMAG, France.

Undergraduate course : Mathieu Cunche, *Security & Privacy*, 21h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Security & Privacy*, 17h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Privacy*, 12h, L3, INSA-Lyon, France.

Master : Cédric Lauradoux, *Introduction to Cryptology*, 30h, M1, University of Grenoble Alpes, France.

Master : Cédric Lauradoux, *Internet Security*, M2, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 20h, M2, Ensimag/University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.

Master : Claude Castelluccia, *Security & Privacy*, 18h, Master MOSIG, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Privacy*, 4h, M2, College de droit University of Grenoble Alpes, France.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Master : Daniel Le Métayer, *Privacy*, 6h, M2 MASH, Université Paris Dauphine, France.

9.2.2. Supervision

PhD defended : Jessye Dos Santos, *Sensor Networks and Privacy*, Claude Castelluccia and Cedric Lauradoux.

PhD defended : Levent Demir, *Trusted module for data outsourcing in the Cloud*, Vincent Roca.

PhD defended : Celestin Matte, *Wi-Fi tracking: Fingerprinting Attacks and Counter-Measures*, Mathieu Cunche.

PhD in progress : Victor Morel, *IoT privacy*, September 2016, Daniel Le Métayer and Claude Castelluccia.

PhD in progress : Mathieu Thiery, *IoT privacy* , September 2016, Vincent Roca.

PhD in progress : Guillaume Celosia, *Wireless Privacy in the Internet of Things* , November 2017, Mathieu Cunche and Daniel.

Intern (M2): Jean-Yves Franceschi, *Accountability of Decision Algorithms*, Daniel Le Métayer Le Métayer.

Intern (M2): Amine Mansour, *Algorithmes d'aide à la décision : des questions éthiques aux défis techniques*, Daniel Le Métayer.

Intern (M2): Jean-Yves Franceschi, *Accountability of Decision Algorithms*, Daniel Le Métayer.

Intern (M2): Coline Boniface, *Laws and Cyberweapons*, Cédric Lauradoux and Claude Castelluccia.

Intern (M2): Jennifer Ridgers, *Surveillance and Social Networks*, Claude Castelluccia and Cédric Lauradoux.

Intern (M1): Iris Lohja, *Mail-Analytics*, Cédric Lauradoux.

9.2.3. Juries

HdR: Melek ONEN, *Security and Privacy for Emerging Technologies*, Eurecom, 12/01/2017, Claude Castelluccia.

PhD: Jessye Dos Santos, *Sensor Networks and Privacy*, 18/10/2016, Claude Castelluccia and Cédric Lauradoux.

PhD: Levent Demir, *Trusted module for data outsourcing in the Cloud*, Université Grenoble Alpes, Grenoble, 07/12/2017, Vincent Roca.

PhD: Celestin Matte, *Wi-Fi tracking: Fingerprinting Attacks and Counter-Measures*, Université Claude Bernard Lyon 1, 8/9/2016, Mathieu Cunche.

PhD: Pierre Laperdrix, *Browser Fingerprinting: Diversity to Augment Authentication and Build Client-side Countermesures*, Rennes University, 03/10/2017, Claude Castelluccia.

PhD: Alban Petit, *Introducing Privacy in Current Web Search Engines*, Insa Lyon, 15/03/2017, Claude Castelluccia..

PhD: Raphaël Gellert, *Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk*, Vrije Universiteit Brussel (VUB), Belgium, 15/06/2017, Daniel Le Métayer.

PhD: Walid Benghabrit, *A formal model for accountability*, IMT Atlantique Bretagne-Pays de la Loire, 27/10/2017, Daniel Le Métayer.

PhD: Raul Pardo, 22 November 2017, Privacy policies for social network – A formal approach, Chalmers University, Göteborg, Sweeden, 22/11/2017, Daniel Le Métayer.

9.3. Popularization

9.3.1. Hearings

D. Le Métayer at the French National Assembly about the implementation of the General Data Protection Regulation (Jan. 2017).

D. Le Métayer at the Conseil national du numérique (CNNum) about the regulation of algorithms (Jul. 2017).

M. Cunche at le Comité Consultatif National d'Ethique (CCNE)[0] (Mar. 2017).

[0] http://www.ccne-ethique.fr/fr

9.3.2. Interviews

M. Cunche by Valentine Faure in Glamour, Donner ses données, juin-juillet 2017.

M. Cunche by Martin Untersinger in lemonde.fr, Apple donne à nouveau des gages en matière de vie privée, 27/09/2017, http://www.lemonde.fr/pixels/article/2017/09/27/apple-donne-a-nouveau-des-gages-en-matiere-de-vie-privee_5192469_4408996.html

M. Cunche by Arnaud Devillard in Sciences et Avenir, Même coupé, le Wi-Fi sous Android peut suivre le téléphone, Oct. 2017, https://www.sciencesetavenir.fr/high-tech/meme-coupe-le-wi-fi-sous-android-peut-suivre-le-telephone_116061

M. Cunche by Camille Gruhier in Que-choisir, Smartphones Android Même une fois le Wi-Fi désactivé, vous êtes pisté, Oct. 2017 https://www.quechoisir.org/actualite-smartphones-android-meme-une-fois-le-wi-fi-desactive-vous-etes-piste-n46076/

M. Cunche by Emilie Brouze in Rue89 - L'Obs, Tu es resté 22 minutes chez l'opticien jeudi. Le centre commercial le sait, le 12 juillet 2017, http://tempsreel.nouvelobs.com/rue89/rue89-nos-vies-connectees/20170711.OBS1939/vous-etes-reste-22-minutes-chez-l-opticien-jeudi-et-le-centre-commercial-le-sait.html

M. Cunche by ZDnet.fr, http://www.zdnet.fr/actualites/android-desactiver-le-wi-fi-n-empeche-pas-d-etre-espionne-39856640.htm

M. Cunche by 01Net, http://www.01net.com/actualites/sur-android-le-wi-fi-peut-vous-tracer-meme-s-il-est-desactive-1245292.html

M. Cunche by l'informaticien, https://www.linformaticien.com/actualites/id/44894/desactiver-le-wifi-pour-eviter-le-flicage-une-protection-illusoire.aspx

M. Cunche by Nextinpact, https://m.nextinpact.com/news/105038-suivi-clients-dans-magasins-question-wi-fi-nest-pas-seule-a-se-poser.htm

C. Lauradoux by Sophie Eremian in Inriality, Quand l'énergie devient intelligente, Oct. 2017, https://www.inriality.fr/environnement/quand-lenergie-devient-intelligente/.

9.3.3. Press articles

D. Le Métayer in Slate, *Designing, explaining and controling algorithms*, in Presidential election, 100 proposals from the research community (Mar. 2017).

D. Le Métayer in Le Monde, *Gouverner les algorithmes pour éviter qu'ils nous gouvernent*, (Nov. 2017).

C. Castelluccia and D. Le Métayer in Inria Analysis note, *Secure electronic documents: is the centralisation of biometric data really inevitable?*, (Feb. 2017).

9.3.4. Conferences

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Exposition Terra Data at Cité des Sciences et de l'Industrie, Apr. 2017.

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Fête de la science at Cité des Sciences et de l'Industrie, Oct. 2017 (broadcasted by Science et Vie TV and animated by l'Esprit Sorcier).

C. Lauradoux, *Email et vie privée: pourquoi utiliser GPG ?*, Cours Master 2, Nov. 2017.

C. Lauradoux, *Mathématiques et la protection de la vie privée*, Olympiades académiques de Mathématiques, May 2017.

C. Lauradoux, *Cryptographie visuelle*, Collège/Lycée Jean Prévost, 01/06/2016.

C. Lauradoux, *Cryptanalyse*, stage MathC2+, 06/2017.

PROSECCO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Prosecco organized the 2nd IEEE European Symposium on Security and Privacy in Paris, 26-28 April 2017. Catalin Hritcu was General Chair, Bruno Blanchet was Finance Chair, and Karthikeyan Bhargavan was Local arrangements Chair.
- Harry Halpin co-chaired the IEEE Security and Privacy on the Blockchain workshop, colocated with IEEE EuroS&P, on 29 April 2017.
- Catalin Hritcu is Artifact Evaluation Co-Chair of POPL 2018
- Catalin Hritcu created a New Workshop on Principles of Secure Compilation (PriSC) colocated with POPL 2017 and 2018. He is PC Chair for PriSC 2018.
- Prosecco organized a Project Everest Workshop at Inria Paris, 2 October 2017
- Prosecco organized an ESOP PC workshop at Inria Paris, 15 December 2017 Workshop at POPL: 13 January 2018, Los Angeles, USA

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Bruno Blanchet was PC member at TAP 2017.
- Harry Halpin was a PC member for ISWC 2017 and WWW 2017.
- Catalin Hritcu was PC member at ESOP 2018 and EuroS&P 2018
- Karthikeyan Bhargavan was a PC member at ACM CCS 2017-18, IEEE S&P 2017-18, POST 2018.

9.1.2.2. Reviewer

- Harry Halpin served as a reviewer for LatinCrypt, AsiaCrypt, JAIST, TCS

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Associate Editor

- of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: Bruno Blanchet

9.1.4. Invited Talks

- Bruno Blanchet gave an invited talk at the workshop on Models and Tools for Security Analysis and Proofs, 2017.
- Bruno Blanchet gave an invited talk at the workshop TLS:DIV (TLS 1.3: Design, Implementation & Verification), 2017.
- Bruno Blanchet gave an invited talk at the workshop TMSP (Trends in Mechanized Security Proofs), 2017.
- Bruno Blanchet gave an invited talk at the Summer Research Institute, EPFL, 2017.
- Harry Halpin gave an invited talk at SPACE 2017
- Harry Halpin gave an invited talk at Conference on Privacy and Data Protection, January 2017.

- Harry Halpin gave an invited talk at RightsCon, March 2017.
- Harry Halpin gave an invited talk at E-CRYPT Cryptosympsium, March 2017.
- Harry Halpin gave an invited talk at La Firma Digital, July 2017.
- Harry Halpin gave an invited talk at Google, October 2017.
- Harry Halpin gave an invited talk at IMMWorld, November 2017.
- Harry Halpin gave an invited talk at Boston University Law School, November 2017.
- Harry Halpin gave an invited talk at University of North Carolina-Chapel Hill, December 2017.
- Harry Halpin gave a keynote talk at Security, and Privacy, and Cryptographic Engineering, December 2017.
- Catalin Hritcu was an invited speaker at TFP 2017
- Catalin Hritcu gave talks at Infoiasi, ESOP PC Workshop, Everest Workshop, TFP (Keynote), FADEx 2017, EuroS&P 2017, Université Clermont Auvergne, University Paris-Sud.
- Karthikeyan Bhargavan gave a keynote at ACNS 2017, Kanazawa, Japan.
- Karthikeyan Bhargavan gave an invited talk at Apple, Cupertino, USA.

9.1.5. Scientific Expertise

- Bruno Blanchet is a member of the specialized temporary scientific committee of ANSM (*Agence nationale de sécurité du médicament et des produits de santé*), on the cybersecurity of software medical devices.
- Karthikeyan Bhargavan advises the TLS working group at the IETF and consults for Mozilla, Apple, and Microsoft Research.
- Catalin Hritcu consilts for Microsoft Research and the DARPA SSITH/HOPE grant.

9.1.6. Research Administration

- Bruno Blanchet is a member of the Inria hiring committee for PhD, post-docs, and *délégations* (*Commision des Emplois Scientifiques*, CES).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master: Catalin Hritcu, Cryptographic protocols: formal and computational proofs, 31.5h equivalent TD, master M2 MPRI, université Paris VII, France
- Doctorat: Catalin Hritcu: Verifying Cryptographic Implementations with F* at Computer-aided security proofs summer school. Aarhus, Denmark, October, 2017
- Doctorat: Catalin Hritcu: Verifying Cryptographic Implementations with F* course at Models and Tools for Cryptographic Proofs summer school, Nancy, France, July 2017
- Master: Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 31.5h equivalent TD, master M2 MPRI, université Paris VII, France
- Master: Karthikeyan Bhargavan, Protocol Verification and Safety, 18h equivalent TD, master ACN, Ecole Polytechnique et Telecom ParisTech, France

9.2.2. Supervision

- PhD: Evmorfia-Iro Bartzia, *A formalization of elliptic curves for cryptography*, Université Paris-Saclay, February 2017. Co-supervised by Pierre-Yves Strub and Karthikeyan Bhargavan.
- PhD in progress: Kenji Maillard, *Semantic Foundations for F**, started January 2017, supervised by Catalin Hritcu and Karthikeyan Bhargavan

- PhD in progress: Jean Karim Zinzindohoue, *A Verified Cryptographic Libary*, supervised by Karthikeyan Bhargavan
- PhD in progress: Nadim Kobeissi, 2015-, *Verified Web Security Applicaitons*, supervised by Karthikeyan Bhargavan
- PhD in progress: Benjamin Beurdouche, 2016-, *Verified Cryptographic Protocols for the Internet of Things*, supervised by Karthikeyan Bhargavan
- PhD in progress: Natalia Kulatova, 2017-, *Verified Hardware Security Devices*, co-supervised by Karthikeyan Bhargavan and Graham Steel
- PhD in progress: Marina Polybelova, 2017-, *Verified Cryptographic Web Applications*, supervised by Karthikeyan Bhargavan
- PhD in progress: Yaëlle Vincont, 2017-, *Software Security: combining fuzzing and symbolic execution for vulnerability detection*, co-supervised by Karthikeyan Bhargavan and Sebastien Bardin

9.2.3. Juries

- Bruno Blanchet was reviewer of Lucca Hirschi's PhD thesis.
- Harry Halpin served on the PhD jury of Evo Busseniers (Vrije Universitat Bruxelles)

9.3. Popularization

- Karthikeyan Bhargavan, Benjamin Beurdouche, Jean Karim Zinzindohoue published a paper in the Communications of the ACM.

TAMIS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Axel Legay was General Chair for KimFest, an event organized for the 60th Birthday of Kim. G. Larsen
- Axel Legay was General Chair for the 1st ACM SAC Conference Track on Software-intensive Systems-of-Systems
- Jean-Louis Lanet was General Chair of Crisis 2017,
- Olivier Zendra was General co-Chair for ARCHI'17, the 9th Summer school on « Architecture des systèmes matériels et logiciels embarqués, et méthodes de conception associées »

10.1.1.2. Member of the Organizing Committees

- Axel Legay coordinated KimFest, an event organized for the 60th Birthday of Kim. G. Larsen

10.1.2. Scientific Events Selection

10.1.2.1. Member of Conference Steering Committees

- Axel Legay is a member of the Steering Committee of the Security summer school organized jointly by pre-GDR security and PEC (Pole d'Excellence Cyber).
- Jean-Louis Lanet has been member of the Steering Committee of Cardis 2017
- Olivier Zendra is a founder and a member of the Steering Committee of ICOOOLPS (International Workshop on Implementation, Compilation, Optimization of OO Languages, Programs and Systems)

10.1.2.2. Chair of Conference Program Committees

- Axel Legay was Scientific chair of the 23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- Axel Legay was the Scientific chair for the 11th International Conference on Risks and Security of Internet and Systems
- Axel Legay was the Scientific chair for the 17th International Conference on Application of Concurrency to System Design (ACSD 2017)
- Olivier Zendra was co-chair with Mario Wolzco of the Program Committee and the Organizing Committee of the 12th Workshop on Implementation, Compilation, Optimization of Object-Oriented Languages, Programs and Systems (ICOOOLPS 2017)

10.1.2.3. Member of the Conference Program Committees

- Axel Legay was a PC member of RV'17, ACSD'17, TACAS'17, CRISIS'17, CMSB'17, SETTA'17, FORMALIZE'17
- Fabrizio Biondi was a PC member of CRISIS'17, MCETECH'17, SAC'17
- Jean-Louis Lanet was PC member of Gramsec'17, Secitc'17, C2SI'17, Mcetech'17 and Afadl'17
- Olivier Zendra was PC member of ICOOOLPS'2017, ARCHI'17 and PEC 2017.

10.1.2.4. Reviewer

- Olivier Zendra was reviewer for MFCS.

- Fabrizio Biondi was a reviewer for CRISIS'17, ESORICS'17, KimFest, LATA'17, MFCS'17, RV'17, MCETECH'17

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Axel Legay is a funder and member of the editorial board of “Foundations for Mastering Changes” journal.
- Annelie Heuser was PC Member/Editorial Board for IACR Transactions On Cryptographic Hardware And Embedded Systems

10.1.3.2. Reviewer - Reviewing Activities

- Axel Legay was reviewer for TCS, TSE, Information and Computation.
- Annelie Heuser was a reviewer for Transactions on Information Forensics & Security, Journal of Cryptographic Engineering, Transactions on Embedded Computing Systems, IEEE Transactions on Very Large Scale Integration Systems
- Jean-Louis was reviewer of Computer and Security journal

10.1.4. Invited Talks

- Axel Legay was an invited speaker for the 11th International Workshop on Reachability Problems.
- Axel Legay was invited speaker for the 43rd International Conference on Current Trends in Theory and Practice of Computer Science
- Fabrizio Biondi was invited speaker for The 12th International Conference on Risks and Security of Internet and Systems
- Florian Dold was invited to the "Re-Imagining Finance" workshop at Columbia Law School in New York City in September 2017.
- Annelie Heuser was invited to a panel discussion for Malicious Software and Hardware in Internet of Things (ACM International Conference on Computing Frontiers
- Jean-Louis Lanet was invited speaker for the INS3PECT workshop, the ROOTS conference, the Conference on Operational Planning, Technological Innovations and Mathematical Applications, the Journée AFSEC. 2017)

10.1.5. Scientific Expertise

- Axel Legay was an expert for the Wallonie Government.
- Axel Legay participated to the CR2 jury for Inria Nice Center as a member of Inria's evaluation committee.
- Olivier Zendra is a CIR expert for the MENESR.
- Olviier Zendra participated to the CR2 jury for Inria Paris Center as a member of Inria's evaluation committee.
- Olivier Zendra is a member of the editorial board and co-author of the “HiPEAC 2017 Vision” [47], as well as the HiPEAC 2019 Vision.

10.1.6. Research Administration

- Axel Legay is a member of Inria's evaluation committee.
- Axel Legay is the Representative for non-permanent staff committees (in charge of postdocs).
- Axel Legay is a member of "club équipe Française de la cyber sécurité"
- Axel Legay is the Britany Region representative in the ECSO organization
- Olivier Zendra is a member of Inria's evaluation committee.
- Olivier Zendra is a member of Inria's workgroup on Inria's social barometer.

- Olivier Zendra was a member of Inria's CNHSCT.
- Olivier Zendra was Head of Inria Nancy's IES Committee (formerly IST).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Master : Axel Legay, Introduction au Model Checking, 36, M2, Université de Bretagne Sud, France
- Master : Axel Legay, Introduction à l'analyse de risques, M2, Université de Bretagne Sud, France
- Licence : Nisrine Jafri , Programmation Java, L3, l'ISTIC, Université Rennes 1, France

10.2.2. Supervision

- PhD in progress : Kevin Bukasa, Démarrage sécurisé, 2015, Jean-Louis Lanet and Axel Legay
- PhD in progress : Mounir Chadli (Rennes 1), On Scheduling and SMC, December 2014, Axel Legay and Saddek Bensalem.
- PhD in progress : Olivier Descourbe, On Code Obfuscation, October 2016, Axel Legay and Fabrizio Biondi.
- PhD in progress : Mike Enescu, On Symbolic Execution for Malware Detection, October 2016, Axel Legay, Flavio Oquendo and Fabrizio Biondi. Terminated on October 2017.
- PhD in progress : Alexandre Gonsalvez, On Obfuscation via crypto primitives, April 2016, Axel Legay and Caroline Fontaine.
- PhD in progress : Nisrine Jafri (Rennes1), On fault Injection detection with MC of Binary code, December 2015, Axel Legay and Jean-Louis Lanet.
- PhD in progress : Razika Lounas, Validation des spécifications formelles de la mise à jour dynamique des applications Java Card, 2010, Mohamed Mezghiche and Jean-Louis Lanet
- PhD in progress: Martin Moreau (Rennes1); On the study of post-quantum cryptography mechanisms (provisory), Axel Legay, Annelie Heuser and Sylvain Guilley
- PhD in progress : Routa Moussaileb, From Data Signature to Behavior Analysis, 2017, Nora Cuppens and Jean-Louis Lanet
- PhD in progress : Tristan Ninet (Rennes 1), Vérification formelle d'une implémentation de la pile protocolaire IKEv2, December 2016, Axel Legay, Romaric Maillard and Olivier Zendra
- PhD in progress: Lamine Nouredine (Rennes1); Developing new packing detection techniques to stop malware propagation, November 2017, Axel Legay and Annelie Heuser.
- PhD in progress : Aurélien Palisse, Observabilité de codes hostiles, 2015, Jean-Louis Lanet
- PhD in progress: Emmanuel Tacheau (Rennes1); Analyse et détection de malwares au moyen de méthodes d'analyse symbolique, September 2017, Axel Legay, Fabrizio Biondi, Alain Fiocco.
- PhD in progress : Aurélien Trulla, Caractérisation de malware Android par suivi de flux d'information et nouvelles techniques d'évasion, 2016, Valerie Viet Triem Tong and Jean-Louis Lanet
- PhD in progress: Alexander Zhdanov (Rennes 1): Modular Automated Syntactic Signature Extraction (MASSE), December 2017, Axel Legay, Fabrizio Biondi, François Déchelle and Olivier Zendra.

10.2.3. Juries

- Axel Legay was a referee for the PhD defense of Xavier Devroye (University of Namur Belgium)
- Axel Legay was a referee for the PhD defense of Quentin Cappart (University of Louvain Belgium)
- Axel Legay was a referee for the PhD defense of Stefan Naujokat (University of Dortmund, Germany)

10.3. Popularization

- Axel Legay participated to the "Forum Cyberstrategia" organized by the ministry of defense, September 2017
- Axel Legay participated to the "Inria Industry days" organized by Inria, October 2017
- Axel Legay participated to the "table ronde sur l'intelligence économique", Rennes November 2017
- Fabrizio Biondi participated to the "Forum International de la Cybersécurité", January 2017
- Fabrizio Biondi participated to the "Forum Cyberstrategia" organized by the ministry of defense, September 2017
- Fabrizio Biondi participated to the "Inria Industry days" organized by Inria, October 2017
- Fabrizio Biondi participated to the "European Cyber Week" organized by IRISA and Bretagne Development Innovation, November 2017