RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2018

Section Dissemination

Edition: 2019-03-07

ALGORITHMICS, COMPUTER ALGEBRA AND CRYPTOLOGY

ARCHITECTURE, LANGUAGES AND COMPILATION

EMBEDDED AND REAL-TIME SYSTEMS

PROOFS AND VERIFICATION

SECURITY AND CONFIDENTIALITY

ARIC Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of Organizing Committees

- Claude-Pierre Jeannerod and Gilles Villard organized the workshop "Structured Matrix Days" (May 14–15, ENS de Lyon, France).
- Fabien Laguillaumie and Damien Stehlé organized the National Codes and Cryptography Days (Journées C2), in Aussois, France.
- Nathalie Revol co-organized the "École Jeunes Chercheurs et Jeunes Chercheuses en Programmation" (June 25–28, ENS de Lyon, France).
- Bruno Salvy is a co-chair of AofA'2019 (Analysis of Algorithms), in Luminy, France.

10.1.2. Scientific Events Selection

10.1.2.1. Member of Conference Program Committees

Chitchanok Chuengsatiansup was in the program committee of CRYPTO 2018.

Gottfried Herold was in the program committee of INDOCRYPT 2018.

Elena Kirshanova was in the program committee of INDOCRYPT 2018.

Benoît Libert was in the program committees of ACNS 2018, SCN 2018, Asiacrypt 2018, PKC 2019.

Jean-Michel Muller was in the program committee of Arith'25 and ASAP'2018.

Alain Passelègue was in the program committee of PKC 2018.

Nathalie Revol was in the program committee of Arith'25, of SCAN 2018 and of Correctness 2018.

Bruno Salvy was in the program committee for AofA'2018, is in the program committee of FPSAC 2019, in the steering committee of AofA and in the scientific committee of OPSFA 2019.

Damien Stehlé was in the program committees of Eurocrypt 2018, SCN 2018, PQCrypto 2018 and PQCrypto 2019. He is in the steering committee of the PQCrypto conference series.

Fabien Laguillaumie was in the program committee of ACISP 2018

10.1.3. Journals

Jean-Michel Muller is associate editor of the IEEE Transactions on Computers.

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

Damien Stehlé is a member of the editorial board of the IACR Journal of Cryptology.

Bruno Salvy and Gilles Villard are members of the editorial board of Journal of Symbolic Computation.

Bruno Salvy is a member of the editorial board of the collection *Text and Monographs in Symbolic Computation* (Springer) and has been for 10 years in the editorial board of the *Journal of Algebra* (section Computational Algebra), which he left in March.

10.1.4. Invited Talks

- Claude-Pierre Jeannerod gave an invited talk *Recent results in fine-grained rounding error analysis* at the SCAN 2018 conference (Tokyo, September 10–15, 2018).

- Jean-Michel Muller gave an invited talk *Arithmétique et précision des calculs sur ordinateurs* at the conference *Tous mesureurs, tous mesurés*, organised by the INSHS and INP Institutes of CNRS, Paris, October 18-19, 2018.
- Benoît Libert gave an invited talk *New Applications of the Lossy Mode of LWE* at the *Chinacrypt 2018* conference, organised by the Chinese Association for Cryptologic Research (CACR) in Chengdu (China) on October 27-28, 2018.
- Damien Stehlé gave an invited talk *On algebraic variants of the LWE problem* at the ICERM workshop *Computational Challenges in the Theory of Lattices*, Providence (RI), on April 23-28, 2018. He also gave an invited talk on the same topic at the *Cryptography and Algorithmic Number Theory* workshop, held in Caen on June 20-22, 2018.
- Elena Kirshanova gave an invited talk *Sieving algorithms for the Shortest Vector Problem* at the *Joint Meeting of the Korean Mathematical Society and the German Mathematical Society*, held in Seoul, Korea, on October 3-6, 2018.
- Gottfried Herold gave an invited talk *Sieving in Practice* at the *Joint Meeting of the Korean Mathematical Society and the German Mathematical Society*, held in Seoul, Korea, on October 3-6, 2018.
- Jean-Michel Muller gave an invited talk *Make computer arithmetic great again* at a panel session on the future of computer arithmetic at Arith-25, 25-27 june 2018.
- Bruno Salvy gave an invited tutorial talk at STACS'2018 on random generation of combinatorial structures.

10.1.5. Leadership within the Scientific Community

Claude-Pierre Jeannerod was member of the scientific committee of JNCF (Journées Nationales de Calcul Formel). He was also a member of the recruitment committee for postdocs and sabbaticals at Inria Grenoble Rhône-Alpes.

Jean-Michel Muller is co-director of the *Groupement de Recherche Informatique Mathématique* (GDR IM) of CNRS; he chaired the HCERES evaluation committees of IRIF (UMR 8243, march 2018) and LIX (UMR 7161, october 2018); he is a member of the Scientific Concil of CERFACS; he participated to the jury of the *Prix La Recherche* award in 2018.

Alain Passelègue is a member of the steering committee of the *Groupe de Travail Codage et Cryptographie* (GT-C2) of the GDR-IM.

Bruno Salvy was a member of the HCERES evaluation committees of IRIF.

Damien Stehlé was a member of the jury for *prix de thèse SIF*.

10.1.6. Research Administration

Gilles Villard is a member of the *Section 6* of the *Comité national de la recherche scientifique*.

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: Nicolas Brisebarre, Approximation Theory and Proof Assistants: Certified Computations, 18h, M2, ENS de Lyon, France

Master: Elena Kirshanova, Cryptanalysis, 18h, M2, ENS de Lyon, France

Master: Guillaume Hanrot, Cryptanalysis, 18h, M2, ENS de Lyon, France

Master: Damien Stehlé, Hard lattice problems, 36h, M2, ENS de Lyon, France

Post-graduate: Damien Stehlé, Hard lattice problems, 45h, Seoul National University, South Korea

Master: Elena Kirshanova, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Alexandre Wallet, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Guillaume Hanrot, Computer Algebra, 10h, M1, ENS de Lyon, France

Master: Bruno Salvy, Computer Algebra, 9h, MPRI, Paris, France

Master: Bruno Salvy, Logic and Complexity, 32h, École polytechnique, France

Master: Vincent Lefèvre, Computer arithmetic, 12h, M2 ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1.

Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 15h, École polytechnique, France

Post-graduate: Bruno Salvy, Experimental Mathematics, 3h, Atelier jeunes chercheurs, St-Flour, France

Post-graduate: Bruno Salvy, Recent algorithms in symbolic summation and integration, 4h, Journées Louis Antoine, Rennes, France

Master: Fabien Laguillaumie, Cryptography, Security, Université Claude Bernard Lyon 1, 150h

Post-graduate : Fabien Laguillaumie, 2-party Computation and Homomorphic Encryption, 1h, École Cyber in Occitanie, France

10.2.2. Supervision

PhD: Fabrice Mouhartem, Privacy-preserving cryptography from pairings and lattices, ENS de Lyon (UdL), 18/10/2018, Benoît Libert

PhD in progress: Radu Titiu, Pseudo-random functions and functional encryption from lattices, ENS de Lyon (UdL), 01/01/2017, Benoît Libert

PhD in progress: Chen Qian, Additively homomorphic encryption and its applications, ENS de Lyon (UdL), 01/09/2016, Benoît Libert

PhD: Weiqiang Wen, Contributions to the hardness foundations of lattice-based cryptography, ENS de Lyon (UdL), 01/09/2015, Damien Stehlé

PhD in progress: Miruna Rosca, Algebraic variants of the LWE problem, ENS de Lyon (UdL), 01/01/2017, Damien Stehlé

PhD in progress: Alice Pellet–Mary, obfuscation cryptanalysis, ENS de Lyon (UdL), 01/09/2016, Damien Stehlé

PhD in progress: Huyen Nguyen, mathematical foundations of lattice-based cryptography, ENS de Lyon (UdL), 01/09/2018, Damien Stehlé

PhD in progress: Florent Bréhard, Outils pour un calcul numérique certifié -Applications aux systèmes dynamiques et à la théorie du contrôle, Ens de Lyon (UdL), 01/09/2016, Nicolas Brisebarre, Mioara Joldeş (CRNS, LAAS) et Damien Pous (CNRS, LIP, Plume)

PhD in progress: Adel Hamdi, Chiffrement fonctionnel pour le traitement de données externes en aveugle, UCBL (UdL) & Orange, 07/12/2017, Sébastien Canard (Orange), Fabien Laguillaumie

PhD in progress: Ida Tucker, Conception de systèmes cryptographiques avancés reposant sur des briques homomorphes, Ens de Lyon (UdL) et Université de Bordeaux, 17/10/2017, Guilhem Castagnos (IMB, Université de Bordeaux), Fabien Laguillaumie

10.2.3. Committees

Benoît Libert: reviewer for the PhD thesis of Pierre-Alain Dupont, ENS, 29/08/2018.

Damien Stehlé: reviewer for the PhD thesis of Thomas Ricosset, ENSEEIHT, 12/11/2018; reviewer for the PhD thesis of Ilaria Chillotti, UVSQ, 17/05/2018; examiner for the PhD thesis of Rachel Player, Royal Holloway University of London, 19/03/2018; president for the PhD thesis of Guillaume Bonnoron, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire, 15/03/2018; jury member for the PhD thesis of Quentin Santos, ENS, 20/12/2018.

Bruno Salvy: member of the HdR committee of Guillaume Chapuy, IRIF, April and of Enrica Duchi, IRIF, November; reviewer for the PhD thesis of Pablo Rotondo, IRIF, September.

Fabien Laguillaumie: reviewer for the PhD thesis of Raphaël Bost, Université Rennes 1, 08/01/2018, Xavier Bultel, Université Clermont Auvergne, 17/05/2018, Vincent Zucca, Sorbonne Université, 25/06/2018, Quentin Santos, ENS, 20/12/2018

Nathalie Revol: examiner for the PhD thesis of Romain Picot, Université Paris 6, 27/03/2018

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Nathalie Revol is a member of the editorial board of interstices; she belongs to the steering committee of MMI (Maison des Mathématiques et de l'Informatique, Lyon)
- Bruno Salvy is "référent chercheur" for the Inria Grenoble Center.

10.3.2. Articles and contents

Nathalie Revol belonged to the working group that elaborated the "7 families of computer science" playcards

10.3.3. Education

Nathalie Revol taught "Dissemination of Scientific Knowledge", 10h, to the 4th year students (between Master and PhD) of ENS de Lyon, France. She has been invited to a panel about "Flashmob" type activities, at ESOF 2018 (EuroScience Open Forum), July 9–14, 2018, Toulouse, France.

Nathalie Revol works with DANE (Délégation Académique au Numérique dans l'Éducation) of Rectorat de Lyon towards educating primary school teachers, by educating educators. She has been invited to present her past activities, using educational robots, at 3es Rencontres Nationales de la Robotique Éducative, October 2–3, Lyon, France.

10.3.4. Interventions

Laurent Grémy and Fabrice Mouhartem gave talks at *Fête de la Science* for a general audience. Nathalie Revol gave talks at *Fête de la Science* for 3 classes (9 years old, 11 years old and 13 years old).

As an incentive for high-school pupils, and especially girls, to choose scientific careers, Nathalie Revol gave talks at Lycée Ella Fitzgerald (Saint-Romain-en-Gal) and Mondial des Métiers (in February 2018). With Jérôme Germoni and Natacha Portier, she organized a day *Filles & Info* in March 2018, gathering about 100 high-school girls of 1e S. She was part of the panel discussing with the audience after the movie "Les figures de l'ombre - Hidden figures" at Comoedia cinema in Lyon in March 2018.

Damien Stehlé received at ENS de Lyon several winning teams of the Alkindi highschool competition. Alice Pellet–Mary and Fabrice Mouhartem gave talks at this event.

AROMATH Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Evelyne Hubert was the general and scientific chair for the conference *Symmetry and Computation* held at the Centre International de Recherche en Mathematiques (Marseille, France) April 3-7.

8.1.1.2. Member of the Organizing Committees

Laurent Busé organized the second "Learning Week" of the ARCADES Network : "Opportunity Recognition" at Inria Sophia Antipolis, March 19-23, 2018.

8.1.2. Scientific Events Selection

8.1.2.1. Reviewer

Bernard Mourrain was reviewer for the conference ISSAC.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

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

Ioannis Emiris is associate editor of the Journal of Symbolic Computation (since 2003) and of Mathematics for Computer Science (since 2017).

Evelyne Hubert is associate editor of the Journal of Symbolic Computation (since 2007) and of Foundations of Computational Mathematics (since 2017).

8.1.3.2. Reviewer - Reviewing Activities

Laurent Busé reviewed for the journal *Linear Algebra and its Applications*, the journal *Computer Aided Geometric Design*, the journal of *Advances in Applied Mathematics*, the *Journal of Computational and Applied Mathematics*, the journal *Applicable Algebra in Engineering, Communication and Computing*, the journal *Computer Aided Design*, the *SIAM Journal on Applied Algebra and Geometry*.

Ioannis Emiris reviewed for the *SIAM Journal on Applied Algebra and Geometry*, the *Symposium of Computational Geometry*.

Bernard Mourrain reviewed for the *Journal of Algebra and its Application*, the journal *Computer Methods in Applied Mechanics and Engineering*, the journal *Computer Aided Geometric Design*, the *Journal of Computational and Applied Mathematics*, the *Journal of Symbolic Computation*, the journal *Mathematics of Computation*. He is also guest editor of the Special Issue of the *Journal Of Symbolic Computation* after MEGA 2017 [24].

Evelyne Hubert reviewed for the *Journal of Symbolic Computation*, the journal *Foundations of Comptutational Mathematics*, and the *Journal of Algebra*.

8.1.4. Invited Talks

Laurent Busé was an invited speaker at the conference "Applied and Computational Geometry" that took place at Loughborough University, Centre for Geometry and Applications, September 12-14, 2018.

Ioannis Emiris was an invited speaker at JRC Ispra, Italy, February 2018, at JK University (and gave a course), Linz, Austria, April-May 2018, at the “2nd Intern. Workshop on Geometry and Machine Learning” , within Computational Geometry Week, Budapest, Hungary, June 2018, at the “Symposium on Discrete Mathematics”, of the German Mathematical Society, Graz, Austria, June 2018, at CHIPSET Training School on Large-Scale Data Mining and Machine Learning for Big Data Analytics (and gave a course), Thessaloniki, 19 September 2018.

Bernard Mourrain was an invited speaker at the Workshop “Structured Matrix Days”, Lyon, 14-15 May, at the International conference on Approximation and Matrix Functions, Lille, May 31 - June 1, at the Workshop “Tensors” (and gave a course), Torino, 10-14 September, at the Workshop “A two-day journey in Computational Algebra and Algebraic Geometry” dedicated to Margherita Roggero, Torino, 27-28 Sep. He was invited at Univ. of Texas, Austin, for a collaboration with Pr. Chandajit Bajaj (29 January - 9 February), an invited participant of the semester on Nonlinear Algebra at ICERM, Providence, RI, USA from 1 to 19 Oct.

Evelyne Hubert gave a keynote lecture at the conference *Symmetry & Computation*, CIRM (Marseille, France) and was invited to give talks at the conference *Algebraic and Geometric Aspects of Numerical Methods for Differential Equations* held at the Mittag-Leffler Institute (Stockholm, Sweden), the *Séminaire différentiel*, jointly organized by Université Versailles St Quentin and Inria SIF, and the conference *Nonlinear Algebra in Applications* held at the Institute for Computational and Experimental Mathematics (Providence, USA).

8.1.5. Scientific Expertise

Evelyne Hubert was part of the hiring committees for the positions of Directeur de Recherche 2ème classe at Inria and for the position of Chargé de Recherche at Inria NGE. As part of the Commission d’Evaluation, she was also part of the promotion committee of Inria researchers (CRHC, DR1, DR0).

Evelyne Hubert was the external reviewer for the promotion of Wei Li to the rank of associate professor at the Chinese Academy of Science (Beijing).

8.1.6. Research Administration

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 Sophia Antipolis centre representative at the “Academic Council” and the “Research Commission” of the University of Nice Sophia Antipolis. He participated to the hiring jury of junior researchers in Inria Sophia Antipolis.

Evelyne Hubert is a member of the Comission d’Evaluation, the national Inria evaluation committee. She is nominated to represent Inria at the Academic Council of the Université Côte d’Azur.

Bernard Mourrain is member of the BCEP (Bureau du Comité des Equipes Projet) of the center Inria- Sophia Antipolis.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Master : Laurent Busé, Geometric Modeling, 27h ETD, M2, EPU of the University of Nice-Sophia Antipolis.
- Master 2: Bernard Mourrain, Symbolic-Numeric Computation, 6h, Master ACSYON, Limoges.

8.2.2. Supervision

PhD in progress: Evangelos Anagnostopoulos, Geometric algorithms for massive data, LAMBDA Marie Skłodowska-Curie RISE Network, started in September 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: Apostolos Chalkis, Sampling in high-dimensional convex regions, started in June 2018, supervised by Ioannis Emiris.

PhD in progress: Emmanouil Christoforou, Geometric approximation algorithms for clustering, Bioinformatics scholarship, started in January 2018, supervised by Ioannis Emiris.

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

PhD: Jouhayna Harmouch, Low rank structured matrix decomposition and applications. Cotutelle Univ. Liban, cosupervised by Houssam Khalil, Mustapha Jazar and Bernard Mourrain. Defended in December.

PhD in progress: Rima Khouja, Tensor decomposition, best approximations, algorithms and applications. Cotutelle Univ. Liban, started in November 2018, cosupervised by Houssam Khalil and Bernard Mourrain.

PhD in progress: Evangelos Bartzos, Algebraic elimination and Distance graphs. ARCADES Marie Skłodowska-Curie ITN, started in June 2016, supervised by Ioannis Emiris.

PhD in progress: Clément Laroche, Algebraic representations of geometric objects. ARCADES Marie Skłodowska-Curie ITN, started in November 2016, supervised by Ioannis Emiris.

PhD in progress: Ioannis Psarros, Dimensionality reduction and Geometric search, Greek scholarship foundation, started in Sep. 2015, supervised by Ioannis Emiris.

PhD in progress: Erick David Rodriguez Bazan, Symmetry preserving algebraic computation. CORDI Inria SAM, started in November 2017, supervised by Evelyne Hubert.

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

8.2.3. Juries

L. Busé was a member of the committee of the PhD of Rémi Bignalet-Cazalet entitled *Géométrie de la projectivisation des idéaux et applications aux problèmes de birationalité*, University Bourgogne Franche-Comté, Dijon, France, October 24th.

I. Emiris was a member of two 3-person supervisory committees of PhD students Anuj Sharma and Emmanouil Kamarianakis, who defended their theses in December 2018, at NK University of Athens, and University of Crete, Greece, respectively.

E. Hubert was a member of the PhD committee of Timothé Pecatte from Ecole Normale Supérieure de Lyon, section informatique : *Bornes Inférieures et Algorithmes de Reconstruction pour des Sommes de Puissances Affines*.

8.3. Popularization

8.3.1. Interventions

- Ioannis Emiris was an invited speaker at “Open Science Days”, Athens, 29 November 2018, and at “Mathematics Education Forum” within the Greek Mathematical Society annual meeting, Athens, December 2018.

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

Paul Zimmermann co-organized two workshops on the development of the iRRAM, GNU MPFR and GNU MPC libraries: one in Dagstuhl in April, with 10 participants, and one in Trier in November, with 12 participants.

Paul Zimmermann also chaired the organizing committee of the EJCIM (*École Jeunes Chercheurs Informatique Informatique Mathématique*) which took place in Nancy in 2018.

10.1.2. Scientific Events Selection

Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

10.1.2.1. Member of steering committees

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

10.1.2.2. Member of the Conference Program Committees

Paul Zimmermann was a member of the program committee of ANTS XIII (Thirteenth Algorithmic Number Theory Symposium, University of Wisconsin, Madison, WI, USA).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Virginie Lallemand is a member of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2018/2019. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE).
- Marine Minier is a guest editor of the special issue of Workshop on Coding and Cryptography (WCC) in the journal Designs, Codes and Cryptography (DCC).

10.1.3.2. 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

- Emmanuel Thomé was invited to give a talk at the ANTS-XIII conference (Madison, WI, USA).
- Marine Minier was invited to give a talk at the Journées Nationales du GT Codage & Cryptographie, Aussois, France.
- Marine Minier was invited to give a talk at Journée “Protection du code et des données, obfuscation & whitebox cryptography”, Paris Saclay, France.
- Paul Zimmermann was invited to give a talk at the topical workshop Celebrating 75 Years of Mathematics of Computation (ICERM, Providence, RI, USA).
- Pierrick Gaudry was invited to give a talk at the 22nd Workshop on Elliptic Curve Cryptography (ECC 2018) in Osaka, Japan.

10.1.5. Research Administration

- Jérémie Detrey chairs the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) of the Inria Nancy – Grand Est research center.
- Pierrick Gaudry is vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine and is a member of the *Conseil Scientifique du GdR IM*.

  He was:
  - member of the CoS, poste MCF number 27MCF1087, Université de Lorraine;
  - member of the CoS, poste PR number 25PR1054, Université de Lorraine;
  - member of the CoS, poste MCF number 25MCF4159, Université de Toulon.
- Marine Minier is a member of Collegium of Science et Techniques of Université de Lorraine. She was:
  - president of the CoS, poste PR number 27PR1057, Université de Lorraine;
  - member of the CoS, poste MCF number 27MCF0403, Université de Grenoble;
  - member of the CoS, poste PR number 270001, École Navale de Brest;
  - member of the CoS, poste MCF number 27MCF4111, Université de Bretagne Sud;
- Pierre-Jean Spaenlehauer is a member of the *commission développement technologique* (CDT) 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.
  - chaired the hiring committee for the junior research positions (CR) at Inria Nancy.
- Marion Videau
  - was a member of the hiring committee for the junior research positions (CR) at Inria Rennes.
- 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.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Cécile Pierrot, *Programmation avancée en Python - TCSS5AC*, 20 eq. TD, L3, Ecole des Mines, Nancy, France.

Master: Cécile Pierrot, *Introduction à Latex*, 3 eq. TD, M1, Ecole des Mines, Nancy, France.

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

Licence, Aurore Guillevic, *Méthodologie de conception et de programmation*, 16 eq. TD (24 TP), L1, Université de Lorraine, Nancy, France.

Formation Continue, Aurore Guillevic, *Introduction à la cryptographie pour enseignants de l’option ISN (informatique et sciences du numérique) en lycée*, 7 eq. TD, Espé de Lorraine (École supérieure du professorat et de l’éducation), Nancy, France.

Licence, Aurore Guillevic, *Introduction to algorithms* (CSE103), 32 eq. TD, L1, École Polytechnique, Palaiseau, France.

Licence, Aurore Guillevic, *Les bases de la programmation et de l’algorithmique* (INF411), 40 eq. TD, 2e année, École Polytechnique, Palaiseau, France.

Master: Marine Minier, *Contrôle d'accès*, 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.

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: Marine Minier, *Mathématiques Discrètes*, 80h eq. TD, L2, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Responsability of the M2 SIRAV *Sécurité Informatique, Réseaux et Architectures Virtuelles*, 30 students: Marine Minier. Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-les-Nancy, France.

Master: Emmanuel Thomé, *Protocoles de sécurité et Vérification* (sub-part dedicated to cryptographic primitives), 8h (lectures) + 6h (tutorial sessions).

10.2.2. Supervision

Ph.D.: Simon Abelard, *Comptage de points de courbes algébriques sur les corps finis et interactions avec les systèmes polynomiaux*, Univ. Lorraine. Defended 7 sept 2018, Pierrick Gaudry & Pierre-Jean Spaenlehauer.

PhD: Svyatoslav Covanov, *Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides*, Université de Lorraine. Defended 5 June 2018, Emmanuel Thomé and Jérémie Detrey.

PhD in progress: Aude Le Gluher, *Analyse algorithmique fine et simulation du crible algébrique*, since Sep. 2018, Pierre-Jean Spaenlehauer and Emmanuel Thomé.

PhD in progress: Simon Masson, *Algorithmique des courbes destinées aux contextes de la cryptographie bilinéaire et post-quantique*, since Jan. 2018, Emmanuel Thomé and Aurore Guillevic.

PhD in progress: Gabrielle De Micheli, *Le logarithme discret dans les corps finis*, since Oct. 2018, Cécile Pierrot et Pierrick Gaudry.

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

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

10.2.3. Juries

Pierrick Gaudry: reviewer of the PhD thesis: *Arithmetric and geometric structures in cryptography* defended by Benjamin Wesolowski, October 2018, EPFL (Switzerland).

Marine Minier:

- reviewer of the PhD thesis: *Trust evaluation in secure architectures* defended by Jean-Baptiste Orfila, July 2018, Université Grenoble Alpes.
- member of the PhD thesis jury: *Security analysis of contactless communication protocols* defended by David Gérault, November 2018, Université Clermont Auvergne.
- member of the PhD thesis jury: *Cryptanalysis of symmetric key algorithms* defended by Colin Chaigneau, November 2018, Université de Versailles.

10.3. Popularization

10.3.1. Articles and contents

- *In books/journals for the general public.*

  Paul Zimmermann coordinated (and largely contributed to) the translation into English of the 2013 book *Calcul mathématique avec Sage*. At the same time, the book was updated to a more recent version of the Sage software tool. The resulting book will be published by SIAM at the end of 2018, while an electronic version will remain available under a Creative Commons license [12].
- *For online publications.* Pierrick Gaudry co-authored a blog article about e-voting and the Belenios tool [13].
- *Interviews in order to popularize.* Cécile Pierrot gave a radio interview at France Bleue about being a cryptographer.
- *Videos.* Cécile Pierrot worked with Accustica, a company which promotes popularization. A portrait was created for the exhibition “Les filles, osez les sciences !” [0]. (video link).

10.3.2. Education

Cécile Pierrot was invited to the exhibition “Les filles, osez les sciences !” to make teachers considers how to deconstruct gender stereotypes in (Computer) Science.

10.3.3. Interventions

Pierrick Gaudry gave a talk about e-voting at the Académie des Sciences.

Emmanuel Thomé gave a talk for students of «classes préparatoires» in Nancy visiting the Inria Nancy research center, on the topic of trapdoored primes in cryptographic standards.

Paul Zimmermann participated in the *Maths-en-jeans* programme, with a class from Lycée Vauban in Luxembourg.

Paul Zimmermann (and Stéphane Glondu from the software development team SED) participated in *Fête de la Science* in October.

Cécile Pierrot co-organized and participated in *Ada Lovelace day*.

Cécile Pierrot gave a talk at Forum de l’Innovation des Armées 2018 about the discrete logarithm problem.

Cécile Pierrot led workshops for secondary-school pupils in Nancy, Reims and Toulouse about research in Computer Science.

[0] Girls, let’s dare to do science!

CASCADE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. Events and Activities

- punctual seminars are organized: https://crypto.di.ens.fr/web2py/index/seminars
- quarterly Paris Crypto Days (https://pariscryptoday.github.io) supported by CryptoCloud and aSCEND
- BibTeX database of papers related to Cryptography, open and widely used by the community (https://cryptobib.di.ens.fr)
- LATCA Bertinoro workshop (http://crypto-events.di.ens.fr/LATCA/)

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. 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 '18 – 16-20 April (San Francisco, California, USA): David Pointcheval
- Eurocrypt '18 – 29 April-3 May (Tel Aviv, Israel): Georg Fuchsbauer and David Pointcheval
- Crypto '18 – 19-23 August (Santa Barbara, USA): Georg Fuchsbauer and Hoeteck Wee
- SCN '18 – 5-7 September (Amalfi, Italy): Georg Fuchsbauer and Romain Gay
- TCC '18 – 11-14 November (Goa, India): Hoeteck Wee

8.1.3. Editorial Boards of Journals

Editor-in-Chief

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

Associate Editor

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

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Master: Michel Abdalla, David Pointcheval, Cryptography, M2, MPRI

- Master: David Pointcheval, Cryptography, M2, ESIEA
- Bachelor: Georg Fuchsbauer, David Pointcheval, Jacques Stern, Hoeteck Wee, Introduction to Cryptology, L3/M1, ENS
- Bachelor: Georg Fuchsbauer, Cryptology, 3rd year, ESGI

8.2.2. Defenses

- PhD: Raphaël Bost, Algorithmes de recherche sur bases de données chiffrées, Univ. Rennes I, January 8th, 2018 (Supervisors: Pierre-Alain Fouque & David Pointcheval)
- PhD: Rafael Del Pino, Efficient Lattice-Based ZeroKnowledge Proofs And Applications, ENS, June 1st, 2018 (Supervisors: Vadim Lyubashevsky & David Pointcheval)
- PhD: Pierre-Alain Dupont, Advanced password-authenticated key exchanges, ENS, August 29th, 2018 (Supervisor: David Pointcheval)
- PhD: Dahmun Goudarzi, Implémentations Sécurisées de Chiffrement par Bloc contre les Attaques Physiques, ENS, September 21st, 2018 (Supervisor: Damien Vergnaud)
- PhD: Michele Minelli, Fully Homomorphic Encryption for Machine Learning, ENS, October 26th, 2018 (Supervisors: Michel Abdalla & Hoeteck Wee)
- PhD: Quentin Santos, Cryptography for Pragmatic Distributed Trust and the Role of Blockchain, ENS, December 20th, 2018 (Supervisor: David Pointcheval)

8.2.3. Supervision

- PhD in progress: Aurélien Dupin, Multi-Party Computations, from 2015, David Pointcheval (with Christophe Bidan, at Rennes)
- PhD in progress: Romain Gay, Functional Encryption, from 2015, Michel Abdalla & Hoeteck Wee
- PhD in progress: Louiza Khati, Disk Encryption Modes, from 2015, Damien Vergnaud
- PhD in progress: Anca Nitulescu, Verifiable Outsourced Computations, from 2015, Michel Abdalla & David Pointcheval
- PhD in progress: Razvan Rosie, Practical Functional Encryption Schemes For the Cloud, from 2015, Michel Abdalla & Hoeteck Wee
- 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)
- PhD in progress: Antoine Plouviez, Privacy and Decentralization, from 2018, Georg Fuchsbauer
- PhD in progress: Quoc Huy Vu, Quantum Cryptography, from 2018, Céline Chevalier

8.2.4. Committees

- PhD Raphaël Bost. *Algorithmes de recherche sur bases de données chiffrées* – Université Rennes I – France – January 8th, 2018: David Pointcheval (Co-supervisor)
- PhD Xavier Bultel. *Mécanismes de délégation pour les primitives de cryptographie à clé publique* – Université Clermont Auvergne – France – May 17th, 2018: David Pointcheval (President)
- PhD Luca Nizzardo. *Cryptographic Techniques for the Security of Cloud and Blockchain Systems* – IMDEA / UPM – Spain – May 24th, 2018: Georg Fuchsbauer (Reviewer)

- PhD Rafael Del Pino. *La cryptographie à base de réseaux* – Ecole Normale Supérieure – France – June 1st, 2018: David Pointcheval (Co-supervisor)
- PhD Pierre-Alain Dupont. *Advanced password-authenticated key exchanges* – Ecole Normale Supérieure – France – August 29th, 2018: David Pointcheval (Supervisor)
- PhD Dahmun Goudarzi. *Implémentations Sécurisées de Chiffrement par Bloc contre les Attaques Physiques* – Ecole Normale Supérieure – France – September 21st, 2018: David Pointcheval (President)
- PhD Cédric Van Rompay. *Protocoles Multi-Utilisateurs de Recherche sur Bases de Données Chiffrées* – Eurecom, Sophia Antipolis, Télécom ParisTech – France – October 4th, 2018: David Pointcheval (President)
- PhD Damien Ligier. *Functional encryption applied to privacy-preserving classification: practical use, performances and security* – CEA, Saclay, IMT Atlantique – France – October 15th, 2018: David Pointcheval (President)
- PhD Fabrice Mouhartem. *Cryptographie protégeant la vie privée à base de couplages et de réseaux* – ENS Lyon – France – October 18th, 2018: David Pointcheval (Reviewer)
- PhD Michele Minelli. *Fully Homomorphic Encryption for Machine Learning* – Ecole Normale Supérieure – France – October 26th, 2018: Michel Abdalla and Hoeteck Wee (Co-supervisors)
- PhD Nadim Kobeissi. *Formal Verification for Real-World Cryptographic Protocols and Implementations* – Inria Paris – France – December 10th, 2018: David Pointcheval (President)
- PhD Quentin Santos. *Cryptography for Pragmatic Distributed Trust and the Role of Blockchain* – Ecole Normale Supérieure – France – December 20th, 2018: David Pointcheval (Supervisor)

DATASHAPE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of Organizing Committees

- F. Chazal co-organised the Tutorial “Machine Learning on Evolutionary Computation” at the IEEE World Congress on Computational Intelligence (WCCI), Rio de Janeiro, July 2018.
- J-D. Boissonnat was a member of the organization committee of the International Conference on Curves and Surfaces, Arcachon, July 2018.
- S. Oudot organized the mini-symposium on topological data analysis and learning at the International Conference on Curves and Surfaces, Arcachon, July 2018.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- S. Oudot was a PC member of the International Symposium on Computational Geometry (SoCG), Budapest, Hungary, June 2018.
- David Cohen-Steiner was a PC member of the Symposium on Geometry Processing (SGP), Paris, France, July 2018, and of Shape Modeling International (SMI), Lisbon, Portugal, June 2018.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

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

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

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

10.1.4. Invited Talks

Frédéric Chazal, Abel Symposium, Geiranger, Norway, June 2018.

Frédéric Chazal, Colloquium de Mathématiques, Math Dept. Amiens, October 2018.

Frédéric Chazal, AI Research Center at National Cheng-Kung University, Taiwan, May 2018.

Frédéric Chazal, National Center for High-performance Computing, Taiwan, May 2018.

Jean-Daniel Boissonnat, Hamilton Mathematics Institute, Trinity College, Dublin, Ireland, June 2018.

Steve Oudot, Workshop “Topological Data Analysis meets Symplectic Topology”, Tel Aviv, Israel, May 2018.

Steve Oudot, Abel Symposium, Geiranger, Norway, June 2018.

Steve Oudot, Banff workshop on multiparameter persistence, Oaxaca, Mexico, August 2018.

Steve Oudot, ICERM, Brown University, Providence, USA, August 2018.

Steve Oudot, workshop on structural inference in high-dimensional models, Moscow, Russia, September 2018.

Clément Maria, Einstein workshop on Geometric and Topological Combinatorics, Freie Universität, Berlin, Germany, October 2018.

10.1.5. Leadership within the Scientific Community

Frédéric Chazal is co-responsible, with S. Arlot (Paris-Sud Univ.), of the “programme Maths-STIC” of the Labex Fondation Mathématique Jacques Hadamard (FMJH).

Frédéric Chazal has been a member of the Scientific council of the french “Agence pour les Mathematiques en Interaction avec l’Entreprise et la Societe (AMIES)” until Dec. 2018.

Frédéric Chazal is a member of the “Comité de pilotage” of the SIGMA group at SMAI.

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

Steve Oudot is co-head (with Luca Castelli-Aleardi) of the GT Géométrie Algorithmique within the GdR Informatique Mathématique.

Steve Oudot is a member of the program committee of the DataIA convergence institute.

10.1.6. Scientific Expertise

- Consulting collaboration for IFPEN to explore potential applications of TDA (from February 2018 to Dec. 2018).

10.1.7. Research Administration

Frédéric Chazal is a member of the Équipe de Direction at Inria Saclay.

Marc Glisse, responsable Raweb pour DataShape

Steve Oudot is vice-president of the Commission Scientifique at Inria Saclay.

Clément Maria is a member of the CDT at Inria Sophia Antipolis-Méditerranée.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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

Master: Frédéric Chazal and Julien Tierny, Topological Data Analysis, 38h eq-TD, M2, Mathématiques, Vision, Apprentissage (MVA), ENS Paris-Saclay, France.

Master: Steve Oudot, Topological data analysis, 45h eq-TD, M1, École polytechnique, France.

Master: Steve Oudot, Data Analysis: geometry and topology in arbitrary dimensions, 24h eq-TD, M2, graduate program in Artificial Intelligence & Advanced Visual Computing, École polytechnique, France.

Undergrad-Master: Steve Oudot, preparatory course for international programming contests, 54h eq-TD, L3/M1, École polytechnique, France.

Summer School on topological data analysis and persistent homology: Steve Oudot, advanced topics, 6h eq-TD, Trento, Italy, June 2018.

Summer School on geometric data: Frédéric Chazal and Marc Glisse, Introduction to Topological Data Analysis, 9h eq-TD, Fréjus, Sept. 2018.

Winter School on Computational Geometry, Amirkabir University of Technology, Tehran, Iran. Course on Delaunay Triangulation of Manifolds, March 2018.

10.2.2. Supervision

PhD : Claire Brécheteau, Statistical aspects of distance-like functions , Defended on September 2018, 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: Jérémy Cochoy, Decomposition and stability of multidimensional persistence modules, Defended on December 10, 2018, Steve Oudot.

PhD in progress: Yitchzak Solomon, Inverse problems in topological data analysis, started September 1st, 2016, Steve Oudot (co-advised by Jeff Brock, Brown University).

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: 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).

PhD in progress: Owen Rouillé, September 2018, co-advised by C. Maria and J-D. Boissonnat.

10.2.3. Juries

J-D. Boissonnat was a member of the committee for the HDR defense of Aurélien Alvarez (Université d'Orléans).

F. Chazal was a member of the PhD defense committee of Jisu Kim (Carnegie Mellon University, advisors: A. Rinaldo and L. Wasserman), Claire Brécheteau (Université Paris-Saclay, advisors: F. Chazal and P. Massart), Hariprasad Kannan (Centrale-Supelec, advisor: N. Paragios), Dorian Nognen (Ecole Polytechnique, advisor: M. Ovsjanikov).

S. Oudot was a member of the Ph.D. defence committee of Tim Ophelders (T.U. Eindhoven, advisors: Bettina Speckmann and Kevin Buchin).

10.3. Popularization

10.3.1. Interventions

- Frédéric Chazal: Fujitsu Forum, “Topological Data Analysis: from academic success to industrial innovation”, Tokyo, Japan, May 2018.
- Frédéric Chazal: “TDA and AI for biomedical applications”, Kaohsiung MEdical Technology Expo, Taiwan, May 2018.

GAIA Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

The GAIA team organized the 2018 edition of the *Computer Algebra in Scientific Computing* (CASC) international workshops series (17–21 September 2018). For more details, see http://www.casc.cs.uni-bonn.de/2018/.

10.1.1.1. General Chair, Scientific Chair

- Since 2018, François Boulier is a *General Chair* of CASC. See http://www.casc-conference.org/.
- A. Quadrat is a member of the *IFAC Technical Committee* “Linear Control Systems”, International Federation of Automatic Control, TC2.2.

10.1.1.2. Member of the Organizing Committees

The GAIA team organized the *Computer Algebra in Scientific Computing* (CASC), University of Lille, 17–21 September 2018.

A. Quadrat is a member of the organization committee of the *Journées Nationales de Calcul Formel* (JNCF), Luminy, France, 22–26/01/2018.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

F. Lemaire was Poster Chair of the *International Symposium on Symbolic and Algebraic Computation* (ISSAC’2018) Poster Session, New York, 16–19/05/2018.

10.1.2.2. Reviewer

- Y. Bouzidi reviewed a publication for ISSAC 2018 and for TDS 2018.
- F. Lemaire reviewed a publication for CASC 2018.
- A. Quadrat reviewed two publications for ISSAC 2018.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

A. Quadrat is associate editor of *Multidimensional Systems and Signal Processing*.

10.1.3.2. Reviewer - Reviewing Activities

A. Quadrat reviewed papers for the journal *Multidimensional Systems and Signal Processing*.

10.1.4. Invited Talks

Y. Bouzidi gave the following talks:

- A Symbolic Approach for Solving Algebraic Riccati Equations, *Journées Nationales de Calcul Formel* (JNCF), CIRM, Marseille - January 22th 2018.
- Parametric study of the critical pairs of linear differential systems with commensurate delays, *Inria DISCO team-project*, Paris - April 30th 2018.
- Using symbolic computation to solve algebraic Riccati equations arising in invariant filtering, *European Control Conference*, Limassol - June 15th 2018.
- A symbolic approach for a parametric H_∞ control problem, *visualization group*, ISCD, Paris - Novembre 30th 2018.

10.1.5. Leadership within the Scientific Community

A. Quadrat co-organized with N. Yeganefar (University of Poitiers) the invited session *New Results in Multidimensional Systems Theory* at the *2018 European Control Conference*, Cyprus, June 12-15, 2018.

R. Ushirobira was co-responsible with Denis Efimov (Non-A Post, Inria) and Gilberto Pin (Electrolux Italia) of a special issue Finite-time estimation, diagnosis and synchronization of uncertain systems for the *European Journal of Control*.

10.1.6. Scientific Expertise

A. Quadrat is a member of the *Bureau du Comité des Equipes-Projets* (BCEP) and of the *Commission des Emplois de Recherche*, Inria Lille - Nord Europe.

A. Quadrat wrote a comparative report for the position “Algorithmische Algebra” (W2), University of Siegen, Germany.

10.1.7. Research Administration

- F. Boulier has been Head of the *Spécialité GIS at Polytech Lille* since June 2018.
- A. Quadrat is in charge with C. Jamroz of the *RaWeb 2018* for Inria Lille – Nord Europe.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Rosane Ushirobira taught around 90h at Polytech Lille and University of Lille (Linear algebra, analysis and logic).

10.2.2. Supervision

PhD: Guillaume Rance, “Commande H_∞ paramétrique et application aux viseurs gyrostabilisés”, University Paris - Saclay, 09/07/2018, Alban Quadrat & Arnaud Quadrat & Hugues Mounier.

PhD in progress: Grace Younes, “Calcul de multiplicités de racines de polynoômes et de quasi-polynoômes”, 01 /10/2018, Alban Quadrat & Yacine Bouzidi & Adrien Poteaux.

Master: Ambroise Fleury (Licence 3 ème année training), “Computation of gcd using AVX”, F. Lemaire.

Master: Guillaume Maitrot (Master 2 training), “Improving the BLINEIDE library with OpenMP”, F. Lemaire.

10.2.3. Juries

F. Boulier was referee of the PhD thesis of G. Rance, University Paris Orsay, 09/07/2018.

A. Quadrat was a jury member of the CRCN Inria 2018 competition for the Lille – Nord Europe center.

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

Since December 2103, R. Ushirobira organize the cycle “30 minutes of science”, a rotating monthly seminar for all researchers at Inria LIlle. On average, 40 people participate in this seminar.

10.3.2. Education

In 2017/2018, Rosane Ushirobira was a referent researcher for *the Math en Jean program* at Arthur Rimbaud College (Villeneuve d’Ascq).

10.3.3. Internal action

Y. Bouzidi, *Symbolic-numeric method for a parametric control problem*, presentation in the *30 minutes of science Inria event*, Lille - January 10th 2018.

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 17th Workshop on Computational Geometry at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

Olivier Devillers and Xavier Goaoc co-organized the Aspag Prospective workshop, April 8-12 2018 in Arcachon.

10.1.1.2. Steering Committees

Monique Teillaud is chairing the Steering Committee of the Symposium on Computational Geometry (SoCG).

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

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

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. Leadership within the Scientific Community

10.1.4.1. Learned societies

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

10.1.5. Research Administration

10.1.5.1. Hiring committees

Sylvain Lazard was the laboratory delegate in a prof (PR) hiring committee at Lorraine Univ. (IUT Charlemagne & Loria).

Monique Teillaud chaired the hiring committee for young researchers (CRCN) of Inria Bordeaux - Sud Ouest.

10.1.5.2. National committees

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

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

10.1.5.3. 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: Head of the Bachelor diploma *Licence Professionnelle Animation des Communautés et Réseaux Socionumériques*, Université de Lorraine. Responsible of Fablab of IUT Charlemagne, Univerasité de Lorraine (since 2018, November). Member of *Comité Information Edition Scientifique* of LORIA.

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 IAEM* (since 2009). Head of the *Mission Jeunes Chercheurs* for Inria national. Head of the Department Algo at LORIA (since 2014). Member of the *Conseil Scientifique* of LORIA (since 2014).

G. Moroz: Member of the *Comité des utilisateurs des moyens informatiques*. Member of the CDT, *Commission de développement technologique*, of Inria Nancy - Grand Est.

M. Pouget is elected at the *Comité de centre*, and is secretary of the board of *AGOS-Nancy*.

M. Teillaud joined the *Conseil de Laboratoire* of LORIA in May. She was a member of the BCP, *Bureau du Comité des Projets* of Inria Nancy - Grand Est until end November.

X. Goaoc is a member of the council of the *Fédération Charles Hermite* since sep. 2018.

10.1.5.4. Websites

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

Licence: Charles Duménil, *Algorithmique et programmation avancée*, 32h, M2, Université de Lorraine, France.

Licence: Laurent Dupont, *Algorithmique*, 15h, L1, Université de Lorraine, France.

Licence: Laurent Dupont, *Web development*, 100h, L2, Université de Lorraine, France.

Licence: Laurent Dupont, *Traitement Numérique du Signal*, 20h, L2, Université de Lorraine, France.

Licence: Laurent Dupont *Web devloppment and Social networks* 100h 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.

Licence: Galatée Hemery, *Programmation*, 64h, L3, École des Mines de Nancy, France.

Master: Vincent Despré, *Algorithmique*, 72h, M1, Polytech Nancy, France.

Master: Vincent Despré, *Systèmes distribués*, 20h, M1, Polytech Nancy, France.

Master: Olivier Devillers, *Modèles d'environnements, planification de trajectoires*, 18h, M2 AVR, Université de Lorraine. https://members.loria.fr/Olivier.Devillers/master/

Master: Olivier Devillers and Marc Pouget, *Computational Geometry*, 24h (academic year 2018-19), M2 Informatique, ENS Lyon https://members.loria.fr/Olivier.Devillers/Master2-ENS-Lyon/.

Master : Xavier Goaoc, *Algorithms and data structures*, 31.5 HETD (academic year 2018-19), M1, École des Mines de Nancy, France

Master : Xavier Goaoc, *Computer architecture*, 31.5 HETD, M1 (academic year 2018-19), École des Mines de Nancy, 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.

PhD in progress: Galatée Hemery, Algorithmic and geometric aspects of inclusion-exclusion, started in Sep. 2018 , supervised by Xavier Goaoc and Éric Colin de Verdière (UPEM).

PhD in progress: Fernand Kuiebove Pefireko, Simulation of random geometric structures, started in Oct. 2018 , supervised by Olivier Devillers.

10.2.3. Juries

O. Devillers was the president of the PhD committee of Tuong-Bach Nguyen (Université de Grenoble).

S. Lazard was a reviewer for the HDR of Yukiko Kenmochi (Université de Marnes-la-Vallée).

G. Moroz was a member of the PhD committee of Guillaume Rance (Université Paris-Sud).

10.3. Popularization

10.3.1. Education

G. Moroz is member of the Mathematics Olympiades committee of the Nancy-Metz academy.

10.3.2. Interventions

L. Dupont participated in several events of popularization of computer science:

Math en Jeans, March 30th, popularization of computer science for high-school students.

ISN day, March 22th, adult continuing education of computer science for high-school teachers.

FabLab14, July 13th, popularization of computer science, general audience.

Ada Lovelace Day 2018, october 9 : popularization of computer science for female high-school students.

GRACE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Member of the Conference Program Committees

- D. Augot was in the program committee of FAB 2018, Foundations and Applications of Blockchain, Los Angeles.
- D. Augot was in the program committee of WTSC 2018, Workshop on Trusted Smart Contracts, Curaçao.
- D. Augot was in the program committee of WAIFI 2018, Workshop on the Arithmetic of Finite Fields, Bergen, Norway.
- D. Augot was in the program committee of BCT 2018, International Workshop on Cryptocurrencies and Blockchain Technology, in conjunction with ESORICS 2018, Barcelona.
- A. Couvreur was in the program committee of the *Journées codes et cryptographie (C2) 2018*.

9.1.1.2. Reviewer

- D. Augot: ISIT 2018 (International Symposium on Information Theory)
- B. Smith: ANTS 2018, Indocrypt 2018, PKC 2019

9.1.2. Journal

9.1.2.1. Member of the Editorial Boards

- F. Morain is member of the editorial board of the *Applicable Algebra in Engineering, Communication and Computing*, Springer.
- With Thomas Johansson, Marine Minier, Faina Soloveva, Victor Zinonviev, D. Augot is guest editor for a special issue of *Designs, Codes and Cryptography*, devoted to WCC2017, Workshop on Coding and Cryptography, St Petersburg, Russia.

9.1.2.2. Reviewer - Reviewing Activities

- A. Couvreur: Designs, Codes and Cryptography, Asiacrypt 2018, IEEE Transactions on information theory, Advances in Mathematics of communication, etc...
- J. Lavauzelle: Designs, Codes and Cryptography (special issue WCC 2017)
- B. Smith: Designs, Codes, and Cryptography, Finite Fields and their Applications, Journal of the London Mathematical Society, Mathematics of Computation,

9.1.3. Invited Talks

- D. Augot was an invited speaker of the Munich Workshop on Coding and Cryptography (MWCC) 2018
- D. Augot was an invited speaker at ACA 2018, Application of Computer Algebra, Santiago de Compostela
- D. Augot was invited at Dasgsthul Seminar 18511, Algebraic Coding Theory for Networks, Storage, and Security, and gave here a talk.
- B. Smith was an invited speaker at the *International Workshop on the Arithmetic of Finite Fields (WAIFI 2018)* (Bergen, Norway).
- B. Smith was an invited speaker at the *Journées Codage et Cryptographie 2018* (Aussois, France).

9.1.4. Industrial Show

- F. Levy-dit-Vehel demoed our Private Information Retrieval protocol at “FIC”, International Security Forum, Lille, January 2018.

9.1.5. Leadership within the Scientific Community

- D. Augot is member of the scientific committee of the C2-CCA seminar, held three or four times a year, with a France wide audience, and which is the seminar of “groupe de travail” C2 “codage et cryptographie” of the GDR IM “groupement de recherche informatique mathématique”.
- D. Augot is leading the scientific committee of the blocksem seminar of Plateau de Saclay.

9.1.6. Scientific Expertise

- A. Couvreur was evaluator for research grants attribution by university of Crete.

9.1.7. Research Administration

- F. Morain is vice-head of the Département d’informatique of Ecole Polytechnique; in charge of years 1 and 2 for Computer Science courses.
- F. Morain is member of the Board of Master Parisien de Recherche en Informatique (MPRI).
- A. Couvreur is member of Inria Saclay *Commission Scientifique*.
- D. Augot was member of the jury for two Inria Grenoble Rhône-Alpes positions
- D. Augot was member of the jury for a position at Institut Mines-Télécom.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence :

- F. Morain, Lectures for INF311: “Introduction à l’informatique”, 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).
- J. Lavauzelle, *Éléments de programmation* (1I002), 13.5h, L1, Université Pierre et Marie Curie, France
- A. Couvreur, INF411 *Introduction à la programmation et à l’algorithmique*, 40h, L3, École Polytechnique, France
- B. Smith, CSE101 *Introduction to Computer Programming*, 36h, L1, École polytechnique, France

Master :

- F. Morain is the scientific leader of the Graduate Degree *Cybersecurity: Threats and Defense* of École Polytechnique.
- A. Couvreur, *Coding theory and application to cryptography*, 20h, M2, MPRI (Université Paris VII, ENS Paris, ENS Cachan, École Polytechnique), France
- F. Morain and A. Couvreur, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique.
- B. Smith, INF568 *Advanced Cryptography*, 36h, M1, École polytechnique
- B. Smith and F. Morain, *Algorithmes arithmétiques pour la cryptologie*, 20h, M2, MPRI (Université Paris VII, ENS Paris, ENS Cachan, École Polytechnique), France
- F. Levy-dit-Vehel, discrete maths, 21h, M1, ENSTA.
- F. Levy-dit-Vehel, cryptography, 24h, M2, ENSTA.

Doctorat :

- A. Couvreur, *Introduction to code based cryptography*, 6 hours. Spring school *Post Scryptum*

9.2.2. Supervision

- PhD : J. Lavauzelle, *Codes à propriétés locales : constructions et applications à des protocoles cryptographiques*, Université Paris Saclay.
- PhD : E. Barelli, *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*, Université Paris Saclay.

9.2.3. Juries

- D. Augot, A. Couvreur, and F. Levy-dit-Vehelwere in the jury of J. Lavauzelle's PhD defense, le 30 novembre 2018, à Palaiseau: *Codes à propriétés locales : constructions et applications à des protocoles cryptographiques*
- D. Augot and A. Couvreur were in the jury of E. Barelli's PhD defense, le 10 décembre 2018 à Palaiseau: *Étude de la sécurité de certaines clés compactes pour le schéma de McEliece utilisant des codes géométriques*
- D. Augot was in in the committee of
  - Victor Cauchois, le jeudi 13 Décembre 2018 à Rennes: *Couches de diffusion linéaires à partir de matrices MDS*
  - Sviat Covanov, le 5 juin 2018 à Nancy: *Multiplication algorithms: algebraic complexity and fast asymptotic methods*
  - Jonathan Detchart, le 5 décembre 2018, à Toulouse: *Optimisation de codes correcteurs d'effacements par application de transformées polynomiales*

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

- D. Augot is member of the "comité de pilotage" the "BART" (Blockchain advanced research and technologies) research initiative, with Institut Mines Télécom and System-X.

9.3.2. Interventions

- D. Augot was interviewed on blockchains by three representatives of the French National Assembly.
- D. Augot was interviewed by "France Stratégie", an institution attached to the Prime Minister to support forward thinking of the French government.
- F. Levy-dit-Vehel demoed our Private Information Retrieval protocol with partitionned locally decodable codes

LFANT Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. 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.

X. Caruso is an editor and one of the founder of the journal *Annales Henri Lebesgue*.

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.

From January 2015 to September 2018 J.-M. Couveignes was a member of the scientific council of the Fondation Mathématique de Paris.

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

8.1.2. Invited Talks

A. Page: *Algorithms for the cohomology of compact arithmetic manifolds and Hecke operators* in the Simons collaboration conference *Arithmetic Geometry, Number Theory, and Computation*, MIT (Boston, US), August 20-24, 2018.

8.1.3. Scientific Expertise

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.

From January 2015 until January 2019, J.-M. Couveignes was 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;

Master : J.-M. Couveignes, *Algorithmic Arithmetic*, 30h, M2, University of Bordeaux, France;

Master : J.-M. Couveignes, *Modules, espaces quadratiques*, 30h, M1, University of Bordeaux, France;

Licence : Jean-Paul Cerri, Algèbre linéaire 2, 51h TD, L2, Université de Bordeaux, France

Licence : Jean-Paul Cerri, Arithmétique et Cryptologie, 24h 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, 60h TD, M1, Université de Bordeaux, France

Master : Jean-Paul Cerri, 3 TER, Université de Bordeaux, France

Licence : Jean Kieffer, Mathématiques pour la biologie, 64h TD, L1, Université de Bordeaux, France

8.2.2. Supervision

PhD: Chloe Martindale, *Isogeny graphs, modular polynomials, and applications*, defended in 2018, supervised by A. Enge and Marco Streng (Universiteit Leiden).

PhD: Antonin Riffaut *Calcul effectif de points spéciaux*, defended in 2018, supervised by Y. Bilu and K. Belabas.

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: 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: Jean Kieffer *Isogénies et endomorphismes de variétés abéliennes*, supervised by D. Robert and A. Page.

Master thesis: Amandine Malonguemfo Teagho *Algorithms for isometries of lattices*, supervised by A. Page.

Master thesis: William Dallaporta *Bhargava's theory and parametrization of algebraic structures*, supervised by K. Belabas.

8.2.3. Juries

X. Caruso has written a report for the doctoral dissertation by Robin Bartlett, King's College in London: *On the reductions of some crystalline representations*.

A. Enge has written a report for the doctoral dissertation by Benjamin Wesolowski, École polytechnique fédérale de Lausanne: *Arithmetic & Geometric Structures in Cryptography*.

A. Enge has written a report for the professorial dissertation by Luca De Feo, Université de Versailles–Saint Quentin: *Exploring Isogeny Graphs*.

8.3. Popularization

8.3.1. Articles and contents

- X. Caruso published an article entitled *Polynômes tordus* in the journal *Au fil des maths de la maternelle à l'université...* edited by APMEP.
- H. Cohen wrote in [28] an introduction to Modular forms, which has been published in the book Notes from the International School on Computational Number Theory.

8.3.2. Education

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.

8.3.3. Interventions

- 24/02/2018 in Olot (Spain), A. Page, with the other participants of Sage Days 93: one day for 20 local high school students to explore mathematical problems.
- 24/05/2018, A. Page: Unithé ou café on the mathematics of wireless communications: *Méthodes algébriques et géométriques pour les communications sans fil : comment l'espace hyperbolique peut-il améliorer vos appels téléphoniques ?*
- 30/05/2018, A. Page: in Poitiers half a day meeting with junior school students who took part in the Al-Kindi competition; introduction to cryptography.
- 27/09/2018 D. Robert and A. Page: demonstration stand on graph-based cryptography at the Inria BSO Party Day.
- 9-11/10/201 A. Page: Fête de la Science at Inria Bordeaux, activity on cryptography (7 groups of students).
- 13/10/2018 D. Robert and A. Page: demonstration stand on graph-based cryptography at the Inria BSO Open Day.
- 11/12/2018 A. Page: talk at the Inria BSO Comité des Projets *Variations arithmétiques et algorithmiques sur le thème << Peut-on entendre la forme d'un tambour? >>*

OURAGAN Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

- Antonin Guilloux is a Co-organizer of the International conference Dynamics of Groups Actions (Cetraro, may 2019) [0]
- Antoine Joux co-organized the Sprint Summer School *Post-Scryptum*[0]
- Antoine-Joux co-organized *Crypto in the quantum age (STIAS)*[0]

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- Antoine Joux was Program Chair of Africacrypt [0]

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Elisha Falbel is a member of the editorial board of *São Paulo Journal of Mathematical Sciences - Springer*
- Antoine Joux is a member of the editorial board of *Designs, Codes and Cryptography*
- Fabrice Rouillier is a member of the editorial board of *Journal of Symbolic Computation*

10.1.3.2. Reviewer - Reviewing Activities

- Antonin Guilloux is reviewer in several journals, including Duke Math Journal.
- Razvan Barbulescu is reviewer for several cryptology conferences including Eurocrypt and WAIFI.

10.1.4. Invited Talks

- Razvan Barbulescu, Cryptography and algorithmic number theory, june 2018, Caen
- Elisha Falbel, Colloquium Heidelberg, June 2018 -Heidelberg -Alemagne
- Elisha Falbel, Representation varieties and geometric structures in low dimensions , July 2018 - Warwick-UK
- Elisha Falbel, Modern Trends in Differential Geometry, July 2018, Sao Paulo- Brazil
- Antonin Guilloux, Computation in Geometric Topology, December 2017 - Warwick - UK.
- Antonin Guilloux, Mahler Measure and values of L-functions, August 2018 - Copenhagen - Denmark.
- Antoine Joux, JFLI (UMI CNRS) / Tokyo university, May 2018, Tokyo https://jfliwp.prod.lamp.cnrs.fr/2018/04/13/jfli-seminar-on-the-mersenne-cryptosystem/
- Antoine Joux, Invited Lecture at the conference *Lattice crypto and algorithms*, May 2018, Bertinoro, Italy
- Antoine Joux, The Mersenne Cryptosystem, Nanyang University, June 2018, Singapore

[0] http://dynamicsgroupactions.imj-prg.fr/fr/68-2/

[0] https://postscryptum.lip6.fr

[0] http://stias.ac.za/events/workshop-on-cryptography-in-the-quantum-age

[0] http://africacrypt2018.aui.ma/commitees.php

10.1.5. Research Administration

- Fabrice Rouillier is a member of the scientific commitee of the Indo French Centre for Applied Mathematics

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Elisha Falbel : courses in Algebra and Analysis, L1 , Sorbonne Université.

Elisha Falbel : Course in Probabiltés, L3, Polytech

Elisha Falbel : Introduction aux surfaces de Riemann, M1, Sorbonne Université.

Antonin Guilloux: Courses in General Mathematics, L1, Sorbonne Université.

Antonin Guilloux: Chair of the Mathematics in L1 at Sorbonne Université; Lead of the renewing of the mathematical courses in L1 at Sorbonne Université for 2019.

Antonin Guilloux: Course in Hyperbolic geometry and character varieties, M2, Sorbonne Université.

Antoine Joux : Course on Techniques in Cryptography and Cryptanalysis, M2, Parisian Master of Research in Computer Science.

Pierre-Vincent Koseleff : Course on Applied Algebra, L3 for undergraduate students (6th semester), Sorbonne Université.

Pierre-Vincent Koseleff : Préparation à l'agrégation de Mathématiques, M2. General Chair and teacher. Sorbonne Université.

Fabrice Rouillier : Course in Algebraic Computations, M1, 24h, Sorbonne Université.

Fabrice Rouillier : Course in "Agrégation Option - C", M2, 31 heures,Sorbonne Université.

Razvan Barbulescu : part of the Course at MPRI Arithmetic algorithms for cryptology 6h

Razvan Barbulescu : 3 projects of cryptology in Python

Razvan Barbulescu : exercice sessions for Algorithmic and complexity 30h

10.2.2. Supervision

PhD in progress : Thomas Espitau, 09/2016, directed by Antoine Joux

PhD in progress : Natalia Kharchenko, 09/2016, directed by Antoine Joux

PhD in progress : Mahya Mehrabdollahei, 09/2018, directed by Antonin Guilloux and Fabrice Rouillier

PhD in progress : Sudarshan Shinde, 09/2016, directed by Razvan Barbulescu and Pierre-Vincent Koseleff

PhD in progress : Robin Timsit, 09/2015, directed by Elisha Falbel

10.2.3. Juries

- Fabrice Rouillier was reviewer of the PhD of Ruben Becker (Universität des Saarlandes)
- Antonin Guilloux, jury of the PhD thesis of Alexandre Bellis - Etude Topologique du Flot Horocyclique Le cas des surfaces Géométriquement Infnies - Supervisor: Françoise Dal'Bo.

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Razvan Barbulescu is *chargé médiation* at IMJ-PRG
- Razvan Barbulescu is a member of the steering commitee of the association *Animath*[0]
- Fabrice Rouillier is *chargé de mission médiation* at Inria Paris
- Fabrice Rouillier is a member of the editorial board of *Interstices*
- Fabrice Rouillier is the president of the association *Animath*

10.3.2. Interventions

- Razvan Barbulescu co-organizes the *Alkindi*[0] competition on crytography (50000 participants)

[0] http://www.animath.fr

[0] http://concours-alkindi.fr/

POLSYS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Dongming Wang was the General Chair of International Conference on Automated Deduction in Geometry (ADG 2018) (Nanning, China, September 11-14, 2018).

Dongming Wang was the General co-Chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019) , Beijing, China, July 15-18, 2019), and the 13th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2018) (Suzhou, China, September 16-19, 2018).

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Elias Tsigaridas was a member of the program committees of the 20th International Workshop on Computer Algebra in Scientific Computing (CASC) 2018.

Mohab Safey El Din was member of the program committee of the 43rd International Symposium on Symbolic and Algebraic Computation (ISSAC) 2018.

Emmanuel Prouff was a member of the programm committee of the Conference on Cryptographic Hardware and Embedded Systems 2018 (CHES), Smart Card Research and Advanced Application Conference (CARDIS) 2018, and Constructive Side-Channel Analysis and Secure Design (COSADE) 2018.

Dongming Wang was a member of the program committee of 13th International Conference on Artificial Intelligence and Symbolic Computation (AISC 2018) (Suzhou, China, September 16-19, 2018) and the 4th International Conference on Numerical and Symbolic Computation (SYMCOMP 2019) (Porto, Portugal, April 11-12, 2019).

9.1.2.2. Reviewer

Mohab Safey El Din was reviewer of the M. Skomra's Phd (CMAP, École polytechnique).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

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

Mohab Safey El Din (with Chee Yap, Courant Inst. NYU) is guest editor of the Journal of Symbolic Computation Special Issue on the 2017 International Symposium on Symbolic and Algebraic Computation.

Dongming Wang is a member of the editorial board of

- 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).

Dongming Wang is a member of the Advisory Board for the journal SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).

Dongming Wang is the Editor-in-Chief for the journal Mathematics in Computer Science (published by Birkhäuser/Springer, Basel).

9.1.4. Invited Talks

Elias Tsigaridas was invited speaker at

- IBM T.J. Watson Research Center, (*Invited talk*) 28 Nov 2018.
- *Applied Algebra Day*. MIT, 17 Nov 2018.
- ICERM, University of Brown, *Main seminar*, Nov, 2018.

Mohab Safey El Din was invited speaker at

- Key Lab on Math. Mechanization, Chinese Academy of Sciences, *Invited talk*.
- Dep. of Math. of Univ. of Tromso, *Invited talk*.
- ICERM, Semester Prog. on Non-linear Algebra, Workshop on Real algebraic geometry and optimization, *Plenary talk*.

Emmanuel Prouff was an invited speaker at

- PANDA 2018 Conference (China) and talked on "Deep Learning for Embedded Security Evaluation".
- COSADE 2018 Conference (Singapur) and talked on "Deep Learning for Embedded Security Evaluation".

9.1.5. Scientific Expertise

Mohab Safey El Din is Chargé de Mission for Computer Science at Sorbonne Univ. (Faculté des Sciences et Ingéniérie).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

Master : Computation Modeling, 38 hours, M1, Sorbonne Université, France.

Master : In charge of Basics of Algebraic Algorithms, 74 hours, M1, Sorbonne Université & Polytech' UPMC, France.

Master : Projects supervision, 6 hours, M1, Sorbonne Université, France.

Licence : Introduction to Algorithmics, 33 hours, L2, Sorbonne Université , France.

Licence : Projects supervision, 10 hours, L2, Sorbonne Université, France.

Licence : In charge of Basics of Programmation 2, 50 hours, L1, Sorbonne Université, France.

Mohab Safey El Din has the following teaching activities:

Master : Computation Modeling, 33 hours, M1, Sorbonne Université, France.

Master : Polynomial System Solving, 40 hours, M1, Sorbonne Université, France.

Master : In charge of the curriculum on Security, Reliability of Performance in Computing, 30 hours, M1, Sorbonne Université , France.

Master : Projects management, 20 hours, M1, Sorbonne Université, France.

Licence : Projects supervision, 10 hours, L2, Sorbonne Université, France.

9.2.2. Supervision

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 : Thi Xuan Vu, Faster algorithms for structured polynomial systems, started in Oct. 2017, Jean-Charles Faugère and Mohab Safey El Din.

PhD in progress : Phuoc Le, Real root classification and polar varieties, started in Oct. 2018, Jean-Charles Faugère and Mohab Safey El Din.

PhD in progress : Simon Landry, Threshold Implementations Against Side Channel Analysis, Emmanuel Prouff.
CIFRE/Contract with ST Micro electronics.

9.2.3. Juries

Mohab Safey El Din was member of the PhD committees of M. Skomra (CMAP, École polytechnique) and T. Weisser (LAAS, CNRS).

SECRET Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- WCC 2019, March 31 - April 5, 2019, St Jacut-de-la-Mer, France: A. Canteaut, program co-chair
- Eurocrypt 2020, Zagreb, Croatia: A. Canteaut, program co-chair
- Workshop on quantum code design and architectures (kick-off meeting of the European project QCDA), November 5-6, 2018, Paris (France): A. Leverrier.

9.1.1.2. Member of the Organizing Committees

- Training School on Symmetric Cryptography and Blockchain: February 19-23, 2018, Torremolinos (Spain): A. Canteaut.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

As a co-editor-in-chief of the journal *IACR Transactions on Symmetric Cryptology*, María Naya-Plasencia served as a program chair of the conference *Fast Software Encryption (FSE)*, held in Bruges March 2018. Gaëtan Leurent will serve as a co-editor-in-chief of *IACR Transactions on Symmetric Cryptology* starting from 2019.

9.1.2.2. Member of the Conference Program Committees

- 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, (M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CT-RSA 2018: April 16-20, 2018, San Francisco, USA (M. Naya-Plasencia);
- Eurocrypt 2018: April 29- May 3, 2018, Tel Aviv, Israel (M. Naya-Plasencia);
- WAIFI 2018: June 14-16, 2018, Bergen, Norway, (L. Perrin)
- SAC 2018: August 13-14, 2018, Calgary, Canada, (G. Leurent);
- Crypto 2018: August 17-19, 2018, Santa Barbara, USA, (M. Naya-Plasencia);
- QCrypt 2018: August 27-31, 2018, Shanghai, China, (A. Leverrier);
- TQC 2018: July 16-18, 2018, Sydney, Australia, (A. Leverrier);
- QTech 2018: September 5-7, 2018, Paris, France, (A. Leverrier);
- SCN 2018: September 5-7, 2018, Amalfi, Italy, (G. Leurent);
- AQIS 2018: September 8-12, 2018, Nagoya, Japan, (A. Leverrier);
- SETA 2018: October 1-6, 2018, Hong-Kong, China, (P. Charpin);
- Asiacrypt 2018: December 02-06, 2018, Brisbane, Australia, (G. Leurent);
- CT-RSA 2019: March 4-8, 2019, San Francisco, USA, (L. Perrin)
- FSE 2019: March 25-28, 2019, Paris, France (C. Boura, A. Canteaut, G. Leurent, M. Naya-Plasencia)

- WCC 2019: March 31 - April 5, 2019, St Jacut-de-la-Mer, France, (A. Canteaut chair, P. Charpin, N. Sendrier, J.P. Tillich);
- PQCrypto 2019: May 8-10, 2019, Chongqing, China, (J.P. Tillich);
- CBC 2019: May 18-19, Darmstadt, Germany, (J.P. Tillich);
- Eurocrypt 2019: May 19-23, 2019, Darmstadt, Germany (C. Boura)
- ISIT 2019: July 7-12, 2019, Paris, France, (J.P. Tillich);
- CHES 2019: August 25-28, 2019, Atlanta, USA, (G. Leurent);
- Eurocrypt 2020: Zagreb, Croatia (A. Canteaut, PC co-chair).

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editor: 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, M. Naya-Plasencia.
- *IACR Transactions on Cryptographic Hardware and Embedded Systems*, associate editors: G. Leurent.
- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich

9.1.3.2. Reviewer - Reviewing Activities

- Remote Referee - step 2- ERC-2018-CoG (A. Canteaut)
- Remote Referee - step 2- ERC-2018-STG (M. Naya-Plasencia)

9.1.4. Invited Talks

- A. Canteaut, *Desperately Seeking Sboxes*, Eurocrypt 2018, Tel Aviv, Israel, April 29 - May 3 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, QUANTALGO Quantum Algorithms and Applications Workshop, 2018, Paris, France, September 25 - 28, 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, CrossFYRE Workshop, 2018, Surrey, UK, September 13 - 14, 2018.
- M. Naya-Plasencia, *New Results on Quantum Symmetric Cryptanalysis*, Journées Nationales 2018 du GDR Informatique Mathématique, Apr 2018, Palaiseau, France
- J.P. Tillich *Schémas cryptographiques à clé publique à base de codes correcteurs proposés à la compétition du NIST*, Journées Nationales 2018 du Pré-GDR Sécurité Informatique, June 1, 2018.

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

- C. Boura, A. Canteaut, J. Jean and V. Suder, *On Sboxes sharing the same DDT*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany
- A. Canteaut *L'insoutenable légèreté du chiffrement*, Journées Scientifiques Inria 2018, June 2018, Bordeaux, France
- A. Canteaut and L. Perrin *On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting*, BFA 2018 - 3rd International Workshop on Boolean Functions and their Applications, Jun 2018, Loen, Norway
- A. Chailloux, *Relativistic commitment and zero-knowledge proofs*, 17th Bellairs Crypto-Workshop 2018, Mar 2018, Holetown, Barbados.
- T. Fuhr, M. Naya-Plasencia and Y. Rotella, *New Results on Modified Versions of Ketje Jr*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany

- G. Leurent, *MDS Matrices with Lightweight Circuits*, The Challenges of Lightweight Cryptanalysis, April 2018, Tel Aviv, Israel.
- G. Leurent, *Security Issues with Small Block Sizes*, Lightweight Crypto Day, April 2018, Tel Aviv, Israel.
- G. Leurent *The Missing Difference Problem*, Flexible Symmetric Cryptography, March 2018, Leiden, Netherlands.
- M. Naya-Plasencia, *Quantum Safe Symmetric Cryptography*, Flexible Symmetric Cryptography Lorentz Center Workshop, 2018, Leiden, Netherlands, March 19 - 23, 2018.
- M. Naya-Plasencia, *Symmetric lightweight primitives: (Design and) Cryptanalysis*, Lightweight Crypto Day, April 2018, Tel Aviv, Israel.
- L. Perrin, *Generalized Feistel Networks with Optimal Diffusion*, Dagstuhl Seminar 18021 Symmetric Cryptography, Jan 2018, Dagstuhl, Germany
- L. Perrin, *S-Box Reverse-Engineering: Boolean Functions, American/Russian Standards, and Butterflies*, CECC 2018 - Central European Conference on Cryptology, Jun 2018, Smolenice, Slovakia.

9.1.5. 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).*
- P. Charpin, N. Sendrier and JP Tillich serve on the steering committee of the WCC conference series.
- A. Leverrier serves on the steering committee of *DIM SIRTEQ* (réseau francilien pour les technologies quantiques).

9.1.6. Research Administration

- A. Canteaut serves as Head of Science of the Inria Paris research center since September 2017.
- A. Canteaut serves on the *Inria Evaluation Committee* since September 2017.
- M. Naya-Plasencia and G. Leurent are members of *Inria Paris CSD 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 as head of the jury for PhD scholarships from EDITE.
- M. Naya-Plasencia serves on the *Comité des usagers du projet "rue Barrault".*

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

- Inria Paris Chargés de recherche: A. Canteaut (vice-chair)
- Inria Chargés de recherche (national selection): A. Canteaut
- ISTIC, Rennes, maître de conférence: M. Naya-Plasencia

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

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

Master: A. Chailloux, *Quantum Information*, 18 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Leverrier, *Quantum information and cryptography*, 18 hours, M2, University Paris-Diderot (MPRI), France;

Master: N. Sendrier, Information theory, 40 hours, M1, UVSQ, MINT, France;

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

Corps des Mines: G. Leurent *Cryptographie symétrique*, 7 hours, Telecom ParisTech, France;

The members of the project-team were also invited to give courses at training schools for PhD students and young researchers:

- A. Canteaut, *Secure building-blocks against differential and linear attacks*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 3 hours.
- A. Canteaut, *Exploiting algebraic properties of block ciphers*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 1.5 hours.
- G. Leurent *How Not to Use a Blockcipher*, Training School on Symmetric Cryptography and Blockchain, Torremolinos, Spain, February 2018. 2.5 hours.
- A. Leverrier, *Security of continuous-variable quantum key distribution*, Secure Quantum Communications School, Baiona, Spain, May 2018.
- M. Naya-Plasencia, *Introduction to Symmetric Cryptography*, Summer School on real-world crypto and privacy, Sibenik, Croatia, June 2018.
- M. Naya-Plasencia, *Lightweight Cryptography*, Summer School on real-world crypto and privacy, Sibenik, Croatia, June 2018.

9.2.2. Supervision

PhD: Sébastien Duval, *Constructions for lightweight cryptography*, Sorbonne Université, October 3, 2018.

PhDs: Yann Rotella, *Finite fields and symmetric cryptography*, Sorbonne Université, September 19, 2018.

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: 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).

PhD in progress: Daniel Coggia, *Cryptanalysis techniques for lightweight ciphers*, since September 2018, supervisors: A. Canteaut and C. Boura.

9.2.3. Juries

- Alex Bredariol Grilo, *Quantum proofs, the Local Hamiltonian problem and applications*; Université Sorbonne Paris Cité, Paris, April 27, 2018, committee: A. Leverrier.
- Vincent Zucca, *Towards efficient arithmetic for Ring-LWE based homomorphic encryption*, Sorbonne Université, June 25, 2018, committee: A. Canteaut (chair);
- Yann Rotella, *Mathématiques discrètes appliquées à la cryptographie symétrique*, Sorbonne Université, September 19, 2018, committee: A. Canteaut (supervisor), M. Naya-Plasencia
- Dahmun Goudarzi, *Secure implementation of block ciphers against physical attacks*, PSL, September 21, 2018, committee: A. Canteaut
- Sébastien Duval, *Constructions pour la cryptographie à bas coût*, Sorbonne Université, October 3, committee: C. Boura, A. Canteaut (supervisor), G. Leurent (supervisor)
- Benjamin Lac, *Cryptographie légère intrinsèquement résistante aux attaques physiques pour l'Internet des objets*, Ecole des Mines de St-Etienne, October 18, 2018, committee: A. Canteaut
- Michele Minelli, *Chiffrement Totalement Homomorphe pour l'Apprentissage Automatique*, Université Paris Sciences et Lettres, October 26, 2018, committee: M. Naya-Plasencia (chair)
- Claire Delaplace, *Algorithmes d'algèbre linéaire pour la cryptographie*, Université de Rennes, November 21, 2018, committee: M. Naya-Plasencia.
- David Gérault, *Security Analysis of Contactless Communication Protocols*, Université Clermont Auvergne, November 27, 2018, committee: M. Naya-Plasencia (reviewer).
- Colin Chaigneau, *Cryptanalyse des Algorithmes de Chiffrement Symétrique*, Université de Versailles, November 28, 2018, committee: M. Naya-Plasencia (reviewer).
- Victor Cauchois, *Couches de Diffusion Lineaires à Partir de Matrices MDS*, Université de Rennes, December 13, 2018, committee: M. Naya-Plasencia.
- Eloi de Chérisey, *Towards a better formalisation of the side-channel threat*, Telecom Paris, December 18, 2018, committee: A. Canteaut (chair).

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

- **Association Animath**: M. Lequesne serves on the board of Animath.
- M. Lequesne is also member of the scientific committee of the French Tournament of Young Mathematicians: redaction of the problems for the competition, jury member (chair of a jury) ; member of the scientific committee of the International Tournament of Young Mathematicians: redaction of the problems for the competition, jury member (chair of a jury) ; Member of the scientific committee of the Correspondances des Jeunes Mathématicien.ne.s: redaction of the problems for the competition.

9.3.2. Articles and contents

- A.Chailloux, *L'algorithme de Shor*, Interstices, Inria, March 2018.
- G. Leurent and M. Naya-Plasencia, *La fragilité inattendue du chiffrement symétrique*, “La Recherche”, November 2018.
- JP Tillich, *Les codes correcteurs*, “La Recherche”, November 2018, p. 45-46.
- A. Canteaut, *La meilleure garantie de sécurité est l'épreuve du temps*, interview to the journal “La Recherche”, November 2018.
- M. Naya-Plasencia, *Symmetric Cryptanalysis: The Foundation of Trust*, Lorentz Center Highlights, 2018, Leiden, Netherlands, Mars 20, 2018.

9.3.3. Education

- **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/. Mathieu Lequesne serves as a co-organizer of the challenge, preparing the three rounds and the final. Together with C. Boura and A. Canteaut, he was also involved in the redaction of the exercises, and in videos for Inria channel on different aspects of cryptography and how to solve problems from the Alkindi challenge: https://www.youtube.com/watch?v=Y-VQBzwEaqQ&t=17s, https://www.youtube.com/watch?v=Mv415zfUFNs&t=3s and https://www.youtube.com/watch?v=8ohEeTPKBwA&t=21s. The best teams from Académie de Paris have been visiting the SECRET project-team in June 2018 https://www.youtube.com/watch?v=EVLHEOWAORc.
- Organization of the event “Rendez-vous des Jeunes Mathématiciennes et Informaticiennes” at Inria Paris (October 22-23) by M. Lequesne, a 2-days camp for 20 high-school girls interested in mathematics and computer science.
- Organization of the International Tournament of Young Mathematicians in Paris, a one-week competition (July 5-12) for 120 high-school students. M. Lequesne served as vice-president of the local organizing committee.

9.3.4. Interventions

- A. Canteaut gave a talk to high-school students at Palais de la Découverte, during the “Semaine des maths” (March 2018) [61];
- A. Canteaut gave the talk during the closing ceremony of “Olympiades nationales de mathématiques” (June 2018) [62];
- A. Canteaut gave a presentation on research in computer science to 10-year children in a school in Paris (Jan. 2018);
- M. Lequesne gave a presentation on code-based cryptography to high-school interns (stagiaires de 3e) (Dec. 2018).

SPECFUN Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

- Alin Bostan is part of the Scientific advisory board of the conference series *Effective Methods in Algebraic Geometry* (MEGA).
- Alin Bostan was a member of the Scientific advisory board of the conference *Algèbre, arithmétique et combinatoire des équations différentielles et aux différences*, CIRM (Luminy, France); ~ 60 participants.
- Alin Bostan is part of the scientific committee of the GDR EFI ("Functional Equations and Interactions") dependent on the mathematical institute (INSMI) of the CNRS. The goal of this GDR is to bring together various research communities in France working on functional equations in fields of computer science and mathematics.
- 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 (and current chair) of the steering committee of the *International Symposium on Symbolic and Algebraic Computation* (ISSAC, 3-year term, 2016–2018).
- Georges Gonthier is a member of the steering committee of the *Certified Programs and Proofs* Conference (CPP).

9.1.1.1. Member of the Organizing Committees

- Alin Bostan co-organizes, with Lucia Di Vizio, the *Séminaire Différentiel* between U. Versailles and Inria Saclay, with a bi-annual frequency (~ 30 participants per event).
- Alin Bostan co-organizes, with Lucia Di Vizio, the working group *Marches dans le quart de plan*, at Institut Henri Poincaré (Paris), with a bi-monthly frequency (~ 15 participants per event).

9.1.2. Scientific Events Selection

9.1.2.1. Reviewer

- Frédéric Chyzak has served as reviewer for the selection of the international conference ISSAC 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Alin Bostan is on the editorial board of the *Journal of Symbolic Computation*.
- Georges Gonthier is on the editorial board of the *Journal of Formalized Reasoning*.

9.1.3.2. Reviewer - Reviewing Activities

- Alin Bostan has served as a reviewer for the journals: *Journal of Symbolic Computation*, *Journal of Combinatorial Theory, Series A*, *Applicable Algebra in Engineering Communications and Computing*, *Minnesota Journal of Undergraduate Mathematics*.
- Frédéric Chyzak has served multiple times as a reviewer for the *Journal of Symbolic Computation*.
- Pierre Lairez has served as a reviewer for the *Journal of Symbolic Computation*, *Journal of the ACM* and *Journal of Physics A*.

9.1.4. Invited Talks

- Alin Bostan has been invited to give a talk at the *Workshop on algebraic and analytic aspects of power series*, Universidade Lisboa, Lisbonne, Portugal, Jan. 2018.
- Alin Bostan has been invited to give a talk at the conference *Algebra, Arithmetic and Combinatorics of Differential and Difference Equations*, CIRM (Luminy), France, May 2018.
- Alin Bostan has been invited to give a talk at the conference *Grands réseaux aléatoires et marches contraintes*, in honor of the 75th birthday of Guy Fayolle, Dijon, France, Aug. 2018.
- Alin Bostan has been invited to give a talk at the conference *Combinatorics and Arithmetic for Physics: special days*, IHES, Bures-sur-Yvette, France, Oct. 2018.
- Frédéric Chyzak was invited invited speaker at the conference *Rencontres Arithmétiques du GDR Informatique Mathématique* (RAIM 2018), Gif-sur-Yvette, France, Nov. 2018.
- Georges Gonthier was a plenary keynote speaker at the *Federated Logic Conference (FLoC 2018)* in Oxford, July 2018.
- Georges Gonthier was invited speaker at the *Workshop on Modular Knowledge (Tetrapod)* during FLoC 2018, Oxford, July 2018.
- Georges Gonthier ws the keynote speaker of the *Future of Mathematical Proofs* workshop at the Heidelberg Laureate Forum, September 2018.

9.1.5. Leadership within the Scientific Community

9.1.5.1. Regular Research Seminar

The team organizes a regular seminar, with roughly 15–20 talks a year. The topics reflect the team's interests: computer algebra, combinatorics, number theory, formal proofs, and related domains. This year, we reduced a bit the number of talks in our seminar, as we have invested much time in setting up a working group with a talk every second week (see 9.1.5.2).

9.1.5.2. Research Working Group

This year we have set up a working group *Marches dans le quart de plan* around the study of walks in the quarter plan, a very active research topic in probability theory and enumerative combinatorics in recent years. The working group is organized at Institut Henri Poincaré, with a regularity of two sessions per month. The original purpose was to read the article “On the Nature of the Generating Series of Walks in the Quarter Plane” by T. Dreyfus, C. Hardouin, J. Roques, M. Singer, published in Invent. Math. this year. But the reality exceeded expectations: the working group attracted a dozen of people, working either in computer science or pure mathematics, who began to interact and a very good dynamic was created. Altogether, sixteen sessions have taken place so far, and we have decided to continue in 2019. From the team, Alin Bostan, Frédéric Chyzak, Guy Fayolle, and Pierre Lairez have given a total of 9 talks to this working group.

9.1.6. Scientific Expertise

- Georges Gonthier participated in a review of the software and algorithms of the Tezos blockchain conducted by the Inria Foundation during Spring 2018.

9.1.7. Research Administration

- Georges Gonthier serves on the Conseil de l'École Doctorale de Mathématiques Hadamard.

9.2. Teaching - Supervision - Juries

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

9.2.1. Teaching

Licence:

Pierre Lairez, *Introduction à l'informatique (INF311)*, TD, 40h, 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 (INF550)*, TD, 18h, M2, École polytechnique, France.

Pierre Lairez, *Les bases de la programmation et de l'algorithmique (INF411)*, TD, 40h, M1, École polytechnique, France.

9.2.2. Juries

- Frédéric Chyzak has been a member of the hiring jury at Inria (Concours CRCN 2018).
- Alin Bostan has served as a referee in the PhD jury of Timothée Pecatte, *Bornes inférieures et algorithmes de reconstruction pour des sommes de puissances affines*, ENS Lyon, July 11, 2018.
- Alin Bostan has served as an examiner in the PhD jury of Boris Djalal, *Formalisations en Coq pour la décision de problèmes en géométrie algébrique réelle*, Inria Sophia Antipolis, December 3, 2018.
- Alin Bostan has served as a member of the monitoring PhD committee of Youssef Abdelaziz, Univ. Paris 6.
- Alin Bostan has served as a member of the monitoring PhD committee of Manon Bertin, Univ. Rouen.

9.3. Popularization

9.3.1. Interventions

- Georges Gonthier testified before the *Mission d'information commune sur les blockchains* of the *Assemblée Nationale* in March.
- Georges Gonthier gave a public lecture and debate on blockchains at the *Institut Diderot* in September, jointly with M. Odonnat (Banque de France).

9.3.2. Internal action

- Georges Gonthier gave a presentation at the *Journées Scientifiques Inria 2018* in Bordeaux.

CAIRN Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- E. Casseau was General Co-Chair of DASIP, Conference on Design and Architectures for Signal and Image Processing, in Porto, Portugal, October 10-12, 2018.
- D. Chillet was General Chair of 10th Workshop on Rapid Simulation and Performance Evaluation: Methods and Tools (RAPIDO), Manchester, United Kingdom, January 22-24, 2018.

10.1.1.2. Member of the Organizing Committees

- E. Casseau is a member of DASIP Steering Committee, Conference on Design and Architectures for Signal and Image Processing.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- O. Sentieys was Track Chair at IEEE NEWCAS and Co-Chair of the D8 Track on Architectural and Microarchitectural Design at IEEE/ACM DATE.

10.1.2.2. 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, IEEE FPT and ARC.
- A. Kritikakou was a member of technical program committee of IEEE RTAS, ECRTS, SAMOS.
- O. Sentieys was a member of technical program committee of IEEE/ACM DATE, IEEE FPL, ACM ENSSys, ACM SBCCI, IEEE ReConFig, CROWNCOM.
- T. Yuki was a member of technical program committee of CGO conference and of Impact workshop.

10.1.3. Member of the Editorial Boards

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

10.1.4. Invited Talks

- D.Chillet gave an invited talk at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Saint Malo, France, January 2018 on "Gestion des fautes au niveau tâche pour architectures MPSoC et Reconfigurables - Aspects multiprocesseur et reconfiguration dynamique".
- C. Killian gave an invited talk at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Saint Malo, France, January 2018 on "Energy-performance tradeoffs in optical Network-on-Chips".
- C. Killian gave an invited talk at OPTICS (4th International Workshop on Optical/Photonic Interconnects for Computing Systems), in conjunction with IEEE/ACM Design Automation and Test in Europe (DATE), Dresden, Germany, march 2018 on "Offline optimization of wavelength allocation and laser to deal with Energy-Performance tradeoffs in nanophotonic interconnects".

- C. Killian gave an invited talk at a thematic day *Photonique sur silicium pour les architectures de calcul* organized by GDR SoC^2, Lyon, France, November 2018 on “Digital architectures to enhance Optical NoCs efficiency”.
- O. Sentieys gave an invited talk at FETCH (École d’hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Saint Malo, France, January 2018 on “Playing with number representations for energy efficiency: an introduction to approximate and stochastic computing”.
- O. Sentieys gave a Keynote at the Third Workshop on Approximate Computing (AxC), in conjunction with IEEE European Test Symposium (ETS), Bremen, Germany, June 2018 on “Playing with number representations and operator-level approximations” [59].
- O. Sentieys gave a tutorial at the Embedded Systems Week (ESWEEK), September 2018 on “A Comprehensive Analysis of Approximate Computing Techniques: From Component- to Application-Level” [55].
- T. Yuki gave an invited talk at TAPAS Workshop, Freiburg im Breisgau, Germany, August 2018 on “Polyhedral Static Analysis for the X10 Language”.

10.1.5. Leadership within the Scientific Community

- E. Casseau is a member of the French National University Council in Signal Processing and Electronics (CNU - Conseil National des Universites, 61ème section) since 2018.
- 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).
- 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.

10.1.6. Scientific Expertise

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching Responsibilities

- C. Wolinski is the Director of ESIR.
- 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, 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.

10.2.2. Teaching

E. Casseau: signal processing, 21h, ENSSAT (L3)

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

E. Casseau: real time design methodology, 57h, ENSSAT (M1)

E. Casseau: computer architecture, 24h, ENSSAT (M1)

E. Casseau: VHDL design, 42h, ENSSAT (M1)

E. Casseau: SoC and high-level synthesis, 33h, Master by Research (SISEA) and ENSSAT (M2)

S. Derrien, optimizing and parallelising compilers, 14h, Master of Computer Science, ISTIC(M2)

S. Derrien, advanced processor architectures, 8h, Master of Computer Science, ISTIC(M2)

S. Derrien, high level synthesis, 20h, Master of Computer Science, ISTIC(M2)

S. Derrien, computer science research projects, 10h, Master of Computer Science, ISTIC(M1)

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

S. Derrien, principles of digital design, 20h, Bachelor of EE/CS, ISTIC(L2)

S. Derrien, computer architecture, 48h, Bachelor of Computer Science, ISTIC(L3)

F. Charot: computer architectures, 16h, ESIR (L3)

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: VLSI integrated circuit design, 24h, ENSSAT (M1)

O. Sentieys: VHDL and logic synthesis, 18h, 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)

10.2.3. Supervision

PhD: Gabriel Gallin, Hardware arithmetic units and cryptoprocessors for hyperelliptic curve cryptography, Nov. 2018, A. Tisserand.

PhD: Aymen Gammoudi, Scheduling and Mapping Strategies for Software Tasks on Energy-Constrained Reconfigurable Architectures, June 2018, D. Chillet, M.Khalgui.

PhD: Jiating Luo, Architectural and Protocol Exploration for 3D Optical Network-on-Chip, Jul. 2018, D. Chillet, C. Killian, S. Le-Beux.

PhD: Mai-Thanh Tran, Towards Hardware Synthesis of a Flexible Radio from a High-Level Language, Nov. 2018, E. Casseau, M. Gautier.

PhD: Van Dung Pham, Architectural Exploration of Network Interface for Energy Efficient 3D Optical Network-on-Chip, Dec. 2018, O. Sentieys, D. Chillet, C. Killian, S. Le-Beux.

PhD: Rafail Psiakis, Performance Optimization Mechanisms for Fault-Resilient VLIW Processors, Dec. 2018, A. Kritikakou, O. Sentieys.

PhD: Simon Rokicki, Hardware acceleration of Dynamic Binary Translation, Dec. 2018, S. Derrien, E. Rohou.

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

PhD in progress: Minyu Cui, Energy-Quality-Time Fault Tolerant Task Mapping on Multicore Architectures, Oct. 2018, E. Casseau, A. Kritikakou.

PhD in progress: Petr Dobias, Energy-Quality-Time Fault Tolerant Task Mapping on Multicore Architectures, Oct. 2017, E. Casseau.

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: Jaechul Lee, Energy-Performance Trade-Off in Optical Network-on-Chip, Dec. 2018, D. Chillet, C. Killian.

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

PhD in progress: Romain Mercier, Fault Tolerant Network on Chip for Deep Learning Algorithms, Oct. 2018, D. Chillet, C. Killian, A. Kritikakou.

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: Davide Pala, Non-Volatile Processors for Intermittently-Powered Computing Systems, Jan. 2018, O. Sentieys, I. Miro-Panades (CEA LETI).

PhD in progress: Joseph Paturel, Design-space exploration of fault-tolerant multicores, Sep. 2018, O. Sentieys, A. Kritikakou.

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.

10.3. Popularization

10.3.1. Articles and contents

Article (in French) about the Embrace project in *Le Mag numérique*: http://www.lemag-numerique.com/2018/01/embrace-vers-radio-hf-numerique-10653

Article in Emergences on “durcir les multi-cœurs contre les rayonnements ionisants”: http://emergences.inria.fr/2018/newsletter-n51/L51-FLODAM

CAMUS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organization

10.1.1.1. Member of Organizing Committees

Philippe Clauss organized the Special Session on Compiler Architecture, Design and Optimization (CADO) of the 16th International Conference on High Performance Computing & Simulation (HPCS 2018), June 2018, Orléans, France.

Cédric Bastoul co-organized HIP3ES 2018 (International Workshop on High Performance Energy Efficient Embedded Systems), in conjunction with the international conference HiPEAC 2018.

10.1.2. Scientific Events Selection

10.1.2.1. Member of Conference Program Committees

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

Cédric Bastoul and Vincent Loechner are part of the program committee of HIP3ES (International Workshop on High Performance Energy Efficient Embedded Systems) in conjunction with the HiPEAC international conference.

Arthur Charguéraud was a member of the program committee for the Symposium on Implementation and Application of Functional Languages (IFL 2018).

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

10.1.2.2. Reviewer

Philippe Clauss has been reviewer for the following conference and workshop: the 2nd International Conference on Computer Science and Application Engineering (CSAE 2018), the International Workshop on Polyhedral Compilation Techniques (IMPACT 2018).
Jens Gustedt has been reviewer for CCGrid 2018.
Arthur Charguéraud has been reviewer for the 30th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA 2018).
Cédric Bastoul has been reviewer for: international conference on Compiler Construction 2018 (CC'2018), the International Workshop on Polyhedral Compilation Techniques (IMPACT 2018), the International Workshop on High Performance Energy Efficient Embedded Systems (HIP3ES 2018).

10.1.3. Journals

10.1.3.1. Member of Editorial Boards

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

10.1.3.2. Reviewer - Reviewing Activities

Bérenger Bramas has been reviewer for the following journal: PPL (Parallel Processing Letters).
Philippe Clauss has been reviewer for the following journals: Engineering Computations, IEEE Transactions on Computers, Future Generation Computer Systems.
Jens Gustedt has been a reviewer for Discrete Applied Mathematics.

Arthur Charguéraud has been reviewer for LFMTP (Logical Frameworks and Meta Languages: Theory and Practice).
Cédric Bastoul has been reviewer for IEEE Transactions on Computers.

10.1.4. Invited Talks

Philippe Clauss has been invited at the Dagstuhl Seminar dedicated to Loop Optimization, March 11-16, 2018. The title of his talk was: *The Polyhedral Model Beyond Static Compilation, Affine Functions and Loops*.

Vincent Loechner has been invited as a speaker at the plenary session of the *journées doctorales du laboratoire d'informatique de l'université de Batna* (Algeria), April 25-26 2018, for a talk entitled *Code Optimizations Using the Polyhedral Model.*

10.1.5. Scientific Expertise

10.1.5.1. 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 clarification report processing, the planning of future versions of the standard and in an subgroup that discusses the improvement of the C memory model.

He was the one of the main forces behind the elaboration of C17, the new version of the C standard that has finally been published by ISO in 2018 [21].

This work on the C programming language also gave rise to the proposal of a language extension, Modular C. It has been used for the implementation of an efficient toolbox for *higher order automatic differenciation*, `arbogast`, see [9], and for the implentation of the work presented in [19].

10.1.5.2. Expertise

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

10.1.6. Research Administration

Jens Gustedt is head of the ICPS team for the ICube lab, and in that function a member of the directory committee of the lab. He is also a member of the local recruiting comission for phds and postdocs of the Inria Center Nancy — Grand Est.

Philippe Clauss and Cédric Bastoul are members of the *Collegium Sciences* of the University of Strasbourg, which is a group of representative scientists providing advice regarding the funding of projects.

Philippe Clauss is a member of the *Bureau du Comité des Projets* of the Nancy Grand Est Inria Center since November 2018. This group of scientists provide assistance to the Director of the Center regarding the recruitment of PhD or post-doc students and Engineers, the funding of projects and provide also some scientific expertise regarding actions of the Center.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence : Philippe Clauss, Architecture des ordinateurs, 18h, L2, Université de Strasbourg, France

Licence : Philippe Clauss, Bases de l'architecture informatique, 22h, L1, Université de Strasbourg, France

Master : Philippe Clauss, Compilation, 84h, M1, Université de Strasbourg, France

Master : Philippe Clauss, Système et programmation temps-réel, 37h, M1, Université de Strasbourg, France

Master : Philippe Clauss, Optimisation et transformations de codes, 31h, M1, Université de Strasbourg, France

Master : Bérenger Bramas, Compilation, 40h, M1, Université de Strasbourg, France

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

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

Licence : Vincent Loechner, responsable pédagogique de la licence professionnelle ARS, L3, Université de Strasbourg, France

Licence : Vincent Loechner, accompagnement et jury de VAE licence professionnelle ARS, L3, Université de Strasbourg, France

Licence : Vincent Loechner, administration système et internet, 40h, L3, Université de Strasbourg, France

Master : Vincent Loechner, langages interprétés, 34h, M1, Université de Strasbourg, France

Master : Vincent Loechner, OS embarqués, 30h, M2, Université de Strasbourg, France

Master : Vincent Loechner, calcul parallèle, 20h, , 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, 28h, Université de Strasbourg, France

Licence : Cédric Bastoul, Computer architecture, 92h, L1, Université de Strasbourg, France

Licence : Cédric Bastoul, Parallel programming, 20h, L3, Université de Strasbourg, France

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

Master : Cédric Bastoul, Introduction to Research, 10h, L2+M1, Université de Strasbourg, France

Licence : Éric Violard, Modèles de Calcul, 29h, L1, Université de Strasbourg, France

Licence : Éric Violard, Programmation fonctionnelle, 85h, L2, Université de Strasbourg, France

Licence : Éric Violard, Architecture des ordinateurs, 54h, L2, Université de Strasbourg, France

Licence : Éric Violard, Logique et programmation logique, 27h, L2, Université de Strasbourg, France

Licence : Éric Violard, Systèmes concurrents, 9h, L3, Université de Strasbourg, France

Licence : Éric Violard, Algorithmique et structures de données, 39h, L3, Université de Strasbourg, France

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

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

10.2.2. Supervision

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

PhD: Mariem Saied, *Automatic Code Generation for Multi-Dimensional Stencil Computations on Distributed-Memory Architectures*, Sep. 2018, Jens Gustedt and Gilles Muller.

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

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

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

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

PhD: Yann Barsamian, *Pic-Vert: A Particle-in-Cell Implementation for Multi-Core Architectures*, Université de Strasbourg, 31 Oct. 2018, Éric 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.

10.2.3. Juries

Philippe Clauss participated to the following PhD committees in 2018:

Date	**Candidate**	**Place**	**Role**
Apr. 25	Mohamed Said MOSLI BOUKSIAA	Université de Paris-Saclay	Reviewer
Nov. 26	Adilla SUSUNGI	University de Paris Sciences et Lettres	Reviewer

Cédric Bastoul participated to the following PhD committees in 2018:

Date	**Candidate**	**Place**	**Role**
Sep. 25	Mariem Said	Université de Strasbourg	President
Dec. 13	Jie Zhao	École Normale Supérieure	Reviewer

10.3. Popularization

10.3.1. Articles and contents

Jens Gustedt is blogging about efficient programming, in particular about the C programming language. To popularize the development of the future C2x standard he has been interviewed for infoQ. He also is an active member of the stackoverflow community a technical Q&A site for programming and related subjects.

10.3.2. Education

A. Charguéraud is a co-organizer of the *Concours Castor informatique*. The purpose of the Concours Castor in to introduce pupils (from *CM1* to *Terminale*) to computer sciences. More information on: http://castor-informatique.fr/.

10.3.3. Interventions

Cédric Bastoul prepared activities and participated to *Fête de la Science* at University of Strasbourg in October 2018.

CASH Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Member of the Organizing Committees

- Laure Gonnord animates the french compilation community since 2010 (http://compilfr.ens-lyon.fr
- Laure Gonnord has coorganised (with other members of the LIP lab) the doctoral school EJCP (École jeunes chercheur.se.s en programmation), in June 2018.

9.1.2. Chair of Conference Program Committees

- Ludovic Henrio was one of the chairs of the **ICE** 2018 workshop (Interaction and Concurrency Experiences), he will also be chairing **ICE** 2019.

9.1.3. Member of the Conference Program Committees

- Christophe Alias is a PC member of **HiP3ES** 2018 – 6th High Performance Energy Efficient Embedded Systems Workshop. He will be a PC member for **COMPAS** 2019 – Conférence d'informatique en Parallélisme, Architecture et Système.
- Matthieu Moy is a PC member of **DUHDe** 2018 — 5th Workshop on Design Automation for Understanding Hardware Designs.
- Laure Gonnord is a PC member of **TAPAS** 2018 - Ninth Workshop on Tools for Automatic Program Analysis, and **VMCAI** 2018 - 19th International Conference on Verification, Model Checking, and Abstract Interpretation. She will be a PC member of **CAV** 2019 Conference on Computer-Aided Verification.
- Ludovic Henrio is a PC member of **4PAD** 2018 (Formal Approaches to Parallel and Distributed Systems), **FASE** 2019 (Fundamental Approaches to Software Engineering). He will be a PC member of **Coordination** 2019 (Conference on Coordination Models and Languages), **ACSD** 2019 (Application of Concurrency to System Design).

9.1.4. Reviewer

- Christophe Alias was reviewer for **HCW** 2018 – 27th International Workshop on Heterogeneity in Computing.
- Matthieu Moy was reviewer for **DATE** 2018 - Design, Automation and Test in Europe, **MCSoC** 2019 - International Symposium on Embedded Multicore/Many-core Systems-on-Chip
- Laure Gonnord was reviewer for **STACS** 2018 - Symposium of Theorical Aspects of Computer Science.
- Ludovic Henrio was reviewer for **FM'2018**.

9.1.5. Journal

9.1.5.1. Reviewer - Reviewing Activities

- Christophe Alias was reviewer for ACM Transactions on Architectures and Code Optimization (**TACO**, ACM) and **Proceedings of the IEEE**.
- Matthieu Moy was reviewer for the Microprocessors and Microsystems Journal (**MICPRO**, Elsevier).
- Ludovic Henrio was reviewer for **JLAMP** (Journal of Logical and Algebraic Methods in Programming), Elsevier.

9.1.6. Invited Talks

- Matthieu Moy presented a talk "Response Time Analysis of Dataflow Applications on a Many-Core Processor with Shared-Memory and Network-on-Chip" for the 30 years of the LIP laboratory, November 2018.
- Laure Gonnord gave two invited talks at the workshop **FAC Days** (Toulouse) and at the International Conference **LOPSTR 2018** "Experiences in designing scalable static analyses".
- Ludovic Henrio gave an invited talk at **HLPP 2018** "An Overview of (some) Active-object Languages" and at **PASS** 2018 workshop "SafePlace: Trustable Virtual Machine Scheduling".

9.1.7. Research Administration

- Laure Gonnord is member of the doctoral commitee of the Inria Grenoble Rhône Alpes center.
- Laure Gonnord is elected member of the LIP council and the Fédération d'Informatique de Lyon council.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

- Christophe Alias, Compilation, CM+TD, 27h, 3A, INSA Centre Val de Loire.
- Laure Gonnord, Algorithmic, C++ Programming, TP: L2, UCBL
- Laure Gonnord, Operating Systems, CM+TD+TP, 24h, L2, UCBL
- Laure Gonnord, Formal Languages, TD+TP, 15h, L3, UCBL
- Laure Gonnord, Logics, TD+TP, 18h, L3, UCBL.
- Matthieu Moy, Concurrent Programming, CM+TD+TP, 57h, L3, UCBL.
- Matthieu Moy, Recursive Programming, TD+TP, 48h, L1, UCBL.
- Matthieu Moy, Software Engineering, CM+TD+TP, 25h, M1, UCBL.
- Matthieu Moy, Git, CM+TP: 12h, L3, UCBL.
- Paul Iannetta, ACM, TD, 32h, L3, ENS de Lyon.
- Julien Braine, Théorie de la programmation, TD/TP, 32h, L3, ENS de Lyon.
- Julien Braine, Projet 1, TP, 32h, L3, ENS de Lyon.

Master:

- Christophe Alias, Compiler optimizations for embedded applications, CM+TD, 27h, 4A, INSA Centre Val de Loire.
- Christophe Alias and Matthieu Moy, Hardware Compilation and Simulation, CM+TD, 36h, M2 Informatique Fondamentale, ENS de Lyon.
- Laure Gonnord, Compilation and Program Analysis, CM, 28h, M1, ENS de Lyon.
- Laure Gonnord, Compilation and program transformations, CM+TD+TP, 35h, M1, UCBL.
- Laure Gonnord, Real Time Systems, CM+TD+TP, 30h, M1, UCBL.
- Laure Gonnord (25%), with Sebastien Mosser, Software Engineering and Compilation, CM+TP, 36h, M2 Informatique Fondamentale, ENS de Lyon.
- Laure Gonnord, Graphs, Complexity, Algorithmics, M1 MEEF (CAPES prepa), CM+TD+TP+oral training, 30h, UCBL.
- Matthieu Moy, Compilation and Program Analysis, TP, 16h, M1, ENS de Lyon.
- Matthieu Moy, Compilation and program transformations, TD+TP, 25h, M1, UCBL.

- Paul Iannetta, Projet intégré, 28h, M1, ENS de Lyon.
- Ludovic Henrio, Distributed Systems: an algorithmic approach, CM+TD, 7h, M2 Specialite IFI (Ingénierie et Fondements de l'Informatique), parcours CSSR, and UBINET, Université de Nice Sophia-Antipolis.

9.2.2. Supervision

- PhD: Amaury Graillat, "Parallel Code Generation of Synchronous Programs for a Many-core Architecture", Univ. Grenoble Alpes, defended on November 16th 2018, supervised by Matthieu Moy (LIP), Pascal Raymond (Verimag) and Benoît Dinechin (Kalray).
- PhD in progress: Gabriel Busnot, "Accélération SystemC pour la co-simulation multi-physique et la simulation de modèles hétérogènes en complexité", Univ. Lyon 1, started in october 2017, supervised by Matthieu Moy (LIP) and Tanguy Sassolas (CEA-LIST).
- PhD in progress: Tristan Delizy, "Dynamic Memory Management For Embedded Non-Volatile Memory", INSA Lyon, started in October 2016, supervised by Guillaume Salagnac (CITI), Tanguy Risset (CITI), Kevin Marquet (CITI) and Matthieu Moy (LIP).
- PhD in progress (from Sept. 2018): Paul Iannetta "Complex data structures scheduling for optimizing compilers", supervised by Lionel Morel (CITI/CEA) and Laure Gonnord (LIP).
- PhD in progress (from Sept. 2018): Julien Braine "Horn Clauses as an Efficient Intermediate Representation for Data Structure Verification", supervised by David Monniaux (CNRS/Verimag) and Laure Gonnord (LIP).
- PhD in progress: Pierre Leca, "Distributed BSP: Active Objects for BSPlib programs", CIFRE Huawei/UNS, started in August 2017, supervised by Gaëtan Hains (Huawei), Wijnand Suijlen (Huawei), Françoise Baude (UNS./I3S), Ludovic Henrio (LIP).

9.2.3. Juries

- Christophe Alias was an expert for the midterm PhD evaluation of Hang Yu from Université Grenoble-Alpes. Hang Yu is supervised by Michaël Perrin and David Monniaux.
- Laure Gonnord was an expert for the midterm PhD evaluation of Sébastien Bonnieux from University Nice Côte d'Azur. Sébastien Bonnieux was supervised by Sébastien Mosser and Mireille Blay-Fornarino.
- Laure Gonnord was reviewer for the PhD of Vincent Botbol from Sorbonne Université entitled "Analyse Statique de programmes concurrents avec variables numériques" and supervised by Emmanuel Chailloux and Tristan Le Gall.
- Laure Gonnord was external jury member for the PhD of Hoby Rakotoarivelo from Université Paris-Saclay entitled "Approche de co-design de noyaux irréguliers sur accélérateurs manycore. Application au cas du remaillage adaptatif pour le calcul intensif" and supervised by Franck Ledoux et Franck Pommereau.
- Laure Gonnord was local jury member for the PhD of Mohammed Amer from Université de Lyon entitled "Centralized Optimization of the Association in IEEE 802.11 Networks" and supervised by Anthony Busson and Isabelle Guérin-Lassous.
- Matthieu Moy was an expert for the midterm PhD evaluation of Joumana Lagha from Ecole centrale de Nantes. Joumana Lagha is supervised by Prof. Olivier H. Roux, Sebastien Faucou and Jean-luc Bechennec.
- Matthieu Moy was reviewer for the Ph.D of Benjamin Rouxel from Université de Rennes 1 entitled "Minimising communication costs impact when scheduling real-time applications on multi-core architectures" and supervised by Isabelle Puaut and Steven Derrien.

9.2.4. Internships

- Bilel Aouadhi, a last year engineer student from Faculté des sciences de Tunis, worked from April 2018 to July 2018 on the implementation of a visualization tool for Data-aware process networks. His was supervised by Christophe Alias and Matthieu Moy, his internship was funded by Université Lyon 1.
- Ligia Novacean, a L3 student from University of Cluj-Napoca (Romania), worked from July 2018 to September 2018 on a DPN-to-C translator for the HLS tool of Xilinx, VivadoHLS. She was supervised by Christophe Alias and Matthieu Moy, her internship was funded by Inria.
- Alexandra Dobre, a L3 student from University of Cluj-Napoca (Romania), worked from July 2018 to September 2018 on the generation of a SystemC simulator from a Data-aware process network. She was supervised by Matthieu Moy and Christophe Alias, her internship was funded by Inria.
- Arthur Gontier, a L3 student from University of Nantes, worked from April 2018 to July 2018 on the formal functional verification of Lustre code with Horn Clauses. He was supervised by Lionel Morel and Laure Gonnord. His internship was founded by the Codas ANR.
- Paul Iannetta, a M2 student from ENS de Lyon, worked from March 2018 to July 2018 on a semantic formalisation of the polyhedral model. He was supervised by Lionel Morel and Laure Gonnord. His internship was founded by the Codas ANR.

9.3. Popularization

9.3.1. Education

- Laure Gonnord is part of the local organisation of the Computer Science preparation for the Agregation examination for future maths teachers (MEEF).

9.3.2. Interventions

- Talk at “Campus du libre” by Matthieu Moy, Doua Lyon, “Pourquoi et comment se lancer dans le libre quand on est étudiant (ou pas) ?”, November 2018.

9.3.3. Internal action

- Café développeur by Matthieu Moy, “Utilisation avancée de Git” at LIRIS (2 sessions), October 2018.

9.3.4. Creation of media or tools for science outreach

- Video “Mon équipe en 180 secondes” by Matthieu Moy for the CASH team.

CORSE Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Yliès Falcone chaired the programme committee of the Software Verification and Testing track of the 2018 ACM Symposium on Applied Computing.
- Yliès Falcone chaired the scientific organization of the 2nd international school on Runtime Verification.

10.1.1.2. Member of the Organizing Committees

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

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Frédéric Desprez: Closer 2018, HPC ’18, SC18 (posters), CEBDA-2018 (with IPDPS’18), CLOUDCOM-2018.
- François Broquedis: IEEE IPDPS 2019, COMPAS 2019
- Fabrice Rastello: ACM SIGPLAN/SIGBED LCTES 2018
- Yliès Falcone: RUME’18, VORTEX’18, 4PAD’18, RV’18, TASE’18, DATE’18

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Frédéric Desprez: IEEE Transaction on Cloud Computing (associate editor)

10.1.4. Invited Talks

- Fabrice Rastello: Saarbruck University: "Automated Derivation of Roofline Performance Limits for Affine Programs"
- Fabrice Rastello: UC Denver: "Automated Derivation of Roofline Performance Limits for Affine Programs"
- Fabrice Rastello: CSU: "Data-Flow/Dependence Profiling for Structured Transformations"
- Frédéric Desprez: CCDSC workshop: SILECS: Super Infrastructure for Large-scale Experimental Computer Science

10.1.5. Leadership within the Scientific Community

- Frédéric Desprez: co-présidence du prix de thèse annuel du GDR Réseaux et Systèmes Distribués (RSD) en collaboration avec l’association ACM SIGOPS France (ASF)
- Frédéric Desprez: Scientific committee of ORAP
- Frédéric Desprez: Technical Committee of GENCI

10.1.6. Scientific Expertise

- Frédéric Desprez: Genci: attribution heures de calcul CT6
- Frédéric Desprez: Groupe de travail “Cloud recherche” du ministère

- Frédéric Desprez: comité des sages IRIT
- Frédéric Desprez: Netherlands Organisation for Scientific Research (NWO), TOP Grants for senior researchers

10.1.7. Research Administration

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master 1: Frédéric Desprez, Parallel Algorithms and Programming, 30 hours, M1 MoSIG and CS, UGA, France

License 3: François Broquedis, Imperative programming using python, 40 hours, Grenoble Institute of Technology (Ensimag)

License 3: François Broquedis, Computer architecture, 40 hours, Grenoble Institute of Technology (Ensimag)

License 3: François Broquedis, C programming, 80 hours, Grenoble Institute of Technology (Ensimag)

Master 1: François Broquedis, Operating systems and concurrent programming, 40 hours, Grenoble Institute of Technology (Ensimag)

Master 1: François Broquedis, Operating Systems Development Project - Fundamentals, 20 hours, Grenoble Institute of Technology (Ensimag)

Master 1: François Broquedis, Operating Systems Project, 20 hours, Grenoble Institute of Technology (Ensimag)

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

Licence: Florent Bouchez Tichadou, Algorithms languages and programming, 113 hours, L2 UGA

Licence: Florent Bouchez Tichadou is responsible of the second year of INF (informatique) and MIN (mathématiques et informatique) students at UGA, eq. 85 hours

Master 1: Yliès Falcone, Proof Techniques and Logic Reminders, MoSIG, 3 hours

Master 1: Yliès Falcone, Programming Language Semantics and Compiler Design, MoSIG and Master informatique, 96 hours

License: Yliès Falcone, Languages and Automata, Univ. Grenoble Alpes, 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)

10.2.2. Supervision

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: Mathieu Stoffel, Static and dynamic approaches for the optimization of the energy consumption associated with applications of the High Performance Computing (HPC) field, February 2018, advised by François Broquedis, Frédéric Desprez, Abdelhafid Mazouz (Atos/Bull) and Philippe Rols (Atos/Bull)

PhD: Ye Xia, Scaling and placement for autonomic management of elasticity of applications in a widely distributed cloud, defended on December 17th 2018, Combining Heuristics for Optimizing and Scaling the Placement of IoT Applications in the Fog, advised by Thierry Coupaye (Orange), Frédéric Desprez, and Xavier Etchevers (Orange)

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

PhD: François Gindraud, Semantics and compilation for a data-flow model with a global address space and software cache coherency. Defended on January 11 2018, advised by Fabrice Rastello and Albert Cohen.

PhD: Thomas Messi Nguelé, Domain Specific Languages for Social Networks Analysis on Multi-Core Architectures, defended on September 15 2018, advised by Maurice Tchuenté (Yaoundé I, LIRIMA) and Jean Francois Méhaut

PhD: Philippe Virouleau, Improving the performance of task-based run-time systems on large scale NUMA machines, defended on June 5 2018, advised by Thierry Gautier (INRIA/AVALON), Fabrice Rastello, and François Broquedis

PhD: Antoine El-Hokayem, Decentralised and Distributed Monitoring of Cyber-Physical Systems, defended on December 18 2018, advised by Yliès Falcone.

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 Francois Méhaut.

PhD in progress: Raphaël Jakse, Interactive Runtime Verification, to be defended in Fall 2019, advised by Jean-François Méhaut and Yliès Falcone.

10.2.3. Juries

10.2.3.1. Frédéric Desprez

- François Gindraud, examiner, *Semantics and compilation for a data-flow model with a global address space and software cache coherency*, PhD, Université Grenoble Alpes, January 11, 2018
- Guillaume Latu, reviewer, *Contribution à la simulation haute-performance et aux méthodes de calcul très extensibles*, HDR, Université de Strasbourg, April 18, 2018
- Bastien Confais, reviewer, *Conception d'un système de partage de données adapté à un environnement de Fog Computing*, PhD, Université de Nantes, July 10, 2018
- Hadrien Croubois, examiner/chair, *Toward an autonomic engine for scientific workflows and elastic Cloud infrastructure*, PhD, ENS Lyon, October 16 2018
- Estelle Dirand, examiner, *Développement d'un système in situ à base de tâches pour un code de dynamique moléculaire classique adapté aux machines exaflopiques*, PhD, Université Grenoble Alpes, November 6, 2018
- Ovidiu Marcu, reviewer, *KerA : A Unified Ingestion and Storage System for Scalable Big Data Processing*, PhD, Insa de Rennes, December 18, 2018
- Mohamed Abderrahim, reviewer, *Conception d'un système de supervision programmable et reconfigurable pour une infrastructure informatique et réseau répartie*, IMT Atlantique, December 19, 2018

10.2.3.2. Fabrice Rastello

- François Gindraud, advisor, *Système distribué à adressage global et cohérence logicielle pourl'exécution d'un modèle de tâche à flot de données*, Université Grenoble Alpes, January 11, 2018
- Johannes Doerfert, reviewer, *Applicable and Sound Polyhedral Optimization of Low-Level Programs*, Universität des Saarlandes, December 19, 2018

- Philippe Virouleau, advisor, *Etude et amélioration de l'exploitation des architectures NUMA à travers des supports exécutifs*, Université Grenoble Alpes, June 5, 2018

10.2.3.3. François Broquedis

- Philippe Virouleau, advisor, *Etude et amélioration de l'exploitation des architectures NUMA à travers des supports exécutifs*, Université Grenoble Alpes, June 5, 2018

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

- Yliès Falcone: Elected member of the Research Council of Univ. Grenoble Alpes.
- Yliès Falcone: Elected member of the Academic Council of Univ. Grenoble Alpes.
- Yliès Falcone: Elected member of the Laboratory Council of the Laboratoire d'Informatique de Grenoble
- Yliès Falcone: Mission Valorisation for the Laboratoire d'Informatique de Grenoble.

PACAP Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Isabelle Puaut is General Chair of the 2018 IEEE Real-Time Systems Symposium (RTSS), held in Nashville, Tennessee (USA) in December 2018.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Sylvain Collange was PC member of DATE 2018 and Compas'2018.
- Pierre Michaud was a member of the program committees of the ICCD 2018 and HPCA 2019 conferences.
- Isabelle Puaut was a member of the program committee of the Euromicro Conference on Real Time Systems (ECRTS) 2018 and 2019, IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2018.
- Isabelle Puaut was a member of the program committee of the "Real-Time and (Networked) Embedded Systems" track of IEEE ETFA 2019.
- Isabelle Puaut was a member of the program committee of the 26th International Conference on Real-Time Networks and Systems, held in Poitiers, October 2018.
- Isabelle Puaut was a member of the program committee of the 18th Workshop on Worst-Case Execution Time Analysis (WCET 2018), held in Barcelona, Spain, July 2018.
- Erven Rohou was a member of the program committee of the International Symposium on Code Generation and Optimization (CGO) 2019.
- Erven Rohou was a member of the program committee of the following international workshops: Euro-EDUPAR, ANDARE, REV-A.
- André Seznec was a member of the ICCD 2018 program committee.

10.1.2.2. Reviewer

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

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Isabelle Puaut is Associate Editor of IEEE Transactions on Computers (IEEE TC) and Springer International Journal of Time-Critical Computing Systems.
- André Seznec is a member of the editorial boards of IEEE Micro and ACM Transactions on Architecture and Compiler Optimization.

10.1.3.2. Reviewer - Reviewing Activities

Members of PACAP routinely review submissions to numerous international journals.

10.1.4. Invited Talks

Members of the PACAP team were invited to present their activity at the RISC-V seminar organized by CEA Grenoble.

André Seznec was an invited speaker at the PER' 18 workshop in Gothenburg, Sweden, May 2018.

André Seznec was an invited speaker at the WOS'18 workshop in Rennes December 2018.

10.1.5. 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).

Isabelle Puaut is member of the steering committee of the Euromicro Conference on Real Time Systems (ECRTS).

10.1.6. Research Administration

Sylvain Collange is a member of the CUMIR (*Commission "Utilisateurs des moyens informatiques Recherche"*).

Isabelle Puaut is member of the Research Council (*Commission Recherche*) of the Université de Rennes 1. 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 Université de Rennes 1).

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

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence: D. Hardy, Real-time systems, 68 hours, L3, Université de Rennes 1, France
- Master: D. Hardy, Operating systems, 53 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Operating systems: concepts and system programming under Linux (SEL), 75 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Operating systems kernels (NOY), 30 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Real-time systems, 55 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Research-oriented student project, 24 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Optimizing and Parallelizing Compilers (OPC), 9 hours, M2, Université de Rennes 1, France
- Master: I. Puaut, Writing of scientific publications, 9 hours, M2 and PhD students, Université de Rennes 1, France
- Master: A. Seznec, Advanced Design and Architectures, 12 hours, M2 SIF, Université de Rennes 1.
- Master: S. Collange, Parallel Programming, 22 hours, M1, Université de Rennes 1, France
- Master: S. Collange, GPU programming, 32 hours, M2, ESIR, France
- Master: S. Collange, Advanced computer architecture, 4 hours, M2, Université de Rennes 1, France
- Master: S. Collange, Advanced CUDA programming, 8 hours, M2, Sorbonne Universités, France

10.2.2. Supervision

PhD: Viet Anh Nguyen, Worst-Case Execution Time (WCET) Estimation for Many-core Architectures, Université de Rennes 1, Feb 2018, advisors I. Puaut (50 %) and D. Hardy (50 %)

Benjamin Rouxel, Code optimizations for WCET calculation on many-core platforms, Dec 2018, advisors I. Puaut (70 %) and S. Derrien from the CAIRN group (30 %).

PhD : Rabab Bouziane, Software-level Analysis and Optimization to Mitigate the Cost of Write Operations on Non-Volatile Memories, Université de Rennes 1, Dec 2018, advisors E. Rohou (70 %) et A. Gamatié from LIRMM (30 %)

PhD : Simon Rokicki, Accélération matérielle pour la traduction dynamique de programmes binaires, Université de Rennes 1, 17 Dec 2018, advisors S. Derrien from CAIRN (70 %) et E. Rohou (30 %)

PhD in progress : Kévin Le Bon, Dynamic Binary Analysis and Optimization for Cyber-Security, started Dec 2018, advisors E. Rohou (30 %), G. Hiet from CIDRE (35 %), F. Tronel from CIDRE (35 %)

PhD in progress : Bahram Yarahmadi, Compiler Optimizations and Worst-Case Energy Consumption, started Feb 2018, advisor E. Rohou

PhD in progress: Arif Ali Ana-Pparakkal, *Dynamic Function Specialization*, Université de Rennes 1, started Feb 2015, advisor E. Rohou

PhD in progress: Kleovoulos Kalaitzidis, Ultrawide Issue Superscalar Processors, Université de Rennes 1, started Dec 2016, advisor A. Seznec

PhD in progress: Niloofar Charmchi, Hardware prefetching and related issues, Université de Rennes 1, started Jan 2017, advisor A. Seznec and S. Collange

PhD in progress: Daniel Rodrigues Carvalho, Towards a compressed memory hierarchy, Université de Rennes 1, started Oct 2017, advisor A. Seznec

10.2.3. Juries

Isabelle Puaut was a member of the following hiring committees (comités de sélection):

- assistant professor position at Université de Rennes 1 on cybersecurity.
- assistant professor at Université de Bretagne Occidentale on cybersecurity in real-time systems
- assistant professor at Université de Nantes on software and hardware for embedded systems

Erven Rohou was a *special expert* for admittance of A. Jimborean as Associate Professor (Swedish *docent*) in Computer Science (Uppsala, Sweden).

Isabelle Puaut was a member of the following committees:

- Mohamed Said Mosli Bouksiaa, Performance variation considered helpful, Université de Paris Saclay, April 2018 (jury member)
- Risat Mahmud Pathan, Design and analysis of real-time parallel and distributed systems. Chalmers University of Technology, Sweden, Oavlönad Docent, Swedish equivalent to HdR, external reviewer.

Erven Rohou was a member of the following committees:

- Antoine Faravelon, Acceleration of memory accesses in Dynamic Binary translation, Université Grenoble Alpes, Oct 2018 (reviewer).

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

Erven Rohou is “correspondant scientifique des relations internationales” for Inria Rennes Bretagne Atlantique. As such he is a member of the Inria COST GTRI (Groupe de Travail “Relations Internationales”).

10.3.2. Articles and contents

PACAP contributed to Inria’s white book on cybersecurity.

10.3.3. Education

Erven Rohou was invited to present the life of a researcher in computer science to middle school students (*Collège de Cesson-Sévigné)*

10.3.4. Interventions

We welcomed a student, grade of 3e (middle-school), for her 3-day observation stay to discover the daily life of researchers in computer science.

AOSTE2 Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

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.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Liliana Cucu-Grosjean has served as PC co-chair for the 14th edition of WFCS 2018 in Imperia, Italy.

Adriana Gogonel has served as PC co-chair for the 12th Junior Researcher Workshop on Real-Time Computing (JWRTC) edition of in Poitiers, France.

10.1.2.2. Member of the Conference Program Committees

Liliana Cucu: RTAS, RTNS, WFCS.

Robert Davis: RTSS, RTAS, RTNS.

Adriana Gogonel: ACM RACS, WMC, JWRTC.

Dumitru Potop Butucaru: ACSD, EMSOFT.

Yves Sorel: DASIP.

10.1.2.3. 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. Member of the Editorial Boards

Liliana Cucu-Grosjean has served as guest editor for the Journal of Real-Time Systems

10.1.3.2. Reviewer - Reviewing Activities

All members of the team are regularly serving as reviewers for the main journals of our domain: Information Processing Letter, Journal of Heuristics, Journal of Real-Time Systems, Journal of Systems Architecture, Journal of Signal Processing Systems, Leibniz Transactions on Embedded Systems, IEEE Transactions on Industrial Informatics, IEEE Transactions on Computers, Theoretical Computer Science.

10.1.4. 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).

10.1.5. Research Administration

Liliana Cucu-Grosjean is member of Inria Evaluation Commission, co-chair of Inria Committee 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: Slim Ben Amor, Machine learning (practice sessions), 20H, M1, ESIEE Engineering School, Noisy-Le-Grand, France.

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

Master: Liliana Cucu-Grosjean, Graph Theory, 32H, M1, ESIEE Engineering School, Cergy Pontoise, France.

Master: Adriana Gogonel, Machine learning, 32H, M1, ESIEE Engineering School, Noisy le Grand, France.

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

Master: Cristian Maxim, Graph Theory, 12H, M1, ESIEE Engineering School, Cergy Pontoise, France.

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

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

10.2.2. Supervision

PhD: Salah-Edinne Saidi, Distributed real-time scheduling for the co-simulation of multiple control models, UPMC, defended April 2018, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel.

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, UPMC, started November 2015, supervised by Dumitru Potop Butucaru.

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, UMPC, started December 2014, co-supervised by Nicolas Pernet (IFPEN) and Yves Sorel.

10.2.3. Juries

Liliana Cucu-Grosjean is PhD examiner for the thesis of Anh Toan Bui Long, University of Poitiers/ENSMA, defended on December 2018.

Dumitru Potop Butucaru is PhD examiner for the thesis of Jad Khatib, Université Pierre et Marie Curie/EDITE, defended September 2018. École doctorale EDITE.

Yves Sorel is Phd examiner for the thesis of Florian Greff, University of Lorraine, defended May 2018.

HYCOMES Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Member of the Conference Program Committees

- Albert Benveniste has served on the Programme Committee of the American Modelica Conference 2018.
- Benoît Caillaud has served on the Steering and Programme Committees of the ACSD'18 conference.
- Khalil Ghorbal has served on the Programme Committee of the Japanese Modelica Conference 2018.

9.1.1.2. Reviewer

- Benoî Caillaud has reviewed papers for the following conferences : ACSD'18,
- Khalil Ghorbal has reviewed papers for the following conferences : Japanese Modelica Conference 2018,

9.1.2. Leadership within the Scientific Community

Albert Benveniste has given a lecture on the Signal synchronous language at Collège de France [9], hosted by Gérard Berry, in the realm of his chair in Computer Science.

9.1.3. Scientific Expertise

- Albert Benveniste is president of the Scientific Council of Orange and member of the Scientific Council of Safran. He has also evaluated grant proposals submitted to the European Research Council.
- Benoît Caillaud has evaluated a grant proposal submitted to the European Research Council. As an Evaluation Committee member, he has served on several Inria hiring and promotion committees (in particular, Senior Researcher at a national level and Junior Researcher in Lillle).

9.1.4. Research Administration

- Albert Benveniste is member of the Burex (Executive Bureau) of the Cominlabs Labex [0].
- Benoît Caillaud is in charge of the IPL ModeliScale [0] national initiative funded by Inria. He is also head of the Programming Languages & Software Engineering department [0] of IRISA.

[0] https://cominlabs.u-bretagneloire.fr/governance

[0] https://team.inria.fr/modeliscale/

[0] http://www.irisa.fr/en/departments/d4-language-and-software-engineering

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

9.2.2. Supervision

PhD: Christelle Kozaily, Structural analysis of nonsmooth dynamical systems, university of Rennes 1, co-supervised by Vincent Acary (Tripop [0] team at Inria Grenoble), Benoît Caillaud and Kahlil Ghorbal, started October 2018.

PhD: Aurélien Lamercerie, Formal analysis of cyber-physical systems requirements expressed in natural language, university of Rennes 1, co-supervised by par Benoît Caillaud et Annie Forêt (SemLIS [0] team of IRISA), started December 2017.

9.2.3. Juries

Benoît Caillaud has been external examiner of Nikolaos Kekatos' PhD, defended at the University of Grenoble Alpes in December 2018. He has also served on the jury of Etienne André's habilitation, defended in June 2018 at University Paris 13.

[0] https://team.inria.fr/tripop/

[0] https://www-semlis.irisa.fr

KAIROS Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Robert de Simone organized the Scientific Program for the yearly Synchron seminar, held in November in Saint-Raphaël. He is also Steering Committee member of IEEE/ACM EmSoft a conference part of Embedded System Week.
- Eric Madelaine is chair of the steering committee of the Int. Symposium on Formal Aspects of Component Software (FACS: http://sevlab.postech.ac.kr/facs18/committees/)
- Frédéric Mallet was track co-chair for DATE 2018.
- Julien Deantoni was track co-chair for IEEE-RIVF (http://rivf2019.udn.vn/).

10.1.1.2. Member of the Organizing Committees

M-A. Peraldi-Frati and R. de Simone organized the Open Workshop Synchron 2018 in Saint-Raphaël.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- M.A Peraldi-Frati is member of the IEEE-RIVF 2019 Program Committee.
- E. Madelaine is member of the PC of FACS'2018, VECoS'2018.
- R. de Simone is PC member for the conference MeMoCode, FDL, and EmSoft.
- Frédéric Mallet. Member of program committee for DATE'18, Euromicro DSD'18, FTSCS'18, FDL'18, TASE'18, Modelsward'18.
- Julien Deantoni is PC member RIVF'19, EXE'18, GEMOC'18, MDebug'18, DSD'18, MoMo'18.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Eric Madelaine is Guest Editor of the Science of Computer Programming special issue for selected papers of the FACS'2014 symposium.
- Frédéric Mallet. Managing Guest Editor for a special issue of Elsevier Science of Computer Programming (SCP).

10.1.3.2. Reviewer - Reviewing Activities

- Eric Madelaine is reviewer for the journals: Science of Computer Programming (SCP), and Journal of Logical and Algebraic Methods in Programming (JLAMP).
- Marie-Agnès Peraldi-Frati : ACM Transactions on CPS, Forte2018.
- Luigi Liquori. Journal reviewer : Fundamenta Informaticae. Conference TPC: NICS'18, ICCE'18
- Frédéric Mallet. Journal reviewer for IEEE Transactions on Computer Aided Design of Integrated Circuits (TCAD), ACM Transactions on Embedded Computing Systems (TECS), ACM Transactions on Design Automation of Electronic Systems (TODAES), Elsevier Computers In Industry.
- Julien Deantoni. Journal reviewer for Software and Systems Modeling (http://www.i3s.unice.fr/~deantoni/SoSyM-review-certificate-Julien-DeAntoni.pdf) and for Computer Languages, Systems & Structures.

10.1.4. Research Administration

- F. Mallet is Deputy Director of UMR I3S Laboratory and as such, member of the ‘comité de direction’, ’conseil de laboratoire’, steering committee of the graduate school (EUR) DS4H.
- Sid Touati is member of the direction committee of I3S laboratory.
- M.A Peraldi-Frati is member of the I3S Laboratory council

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence : Sid TOUATI, Fondement machine, 75 heures eq TD, L1 informatique, Université Côte d’Azur.

Licence : Sid TOUATI, Architecture machine, 45 heures eq TD, L3 informatique, Université Côte d’Azur.

Licence : Sid TOUATI, Compilation, 33 heures eq TD, L3 informatique, Université Côte d’Azur.

Master: Sid TOUATI, Architectures et logiciels hautes performances, 81 heures eq TD, Master 1 informatique, Université Côte d’Azur.

Master international: Sid TOUATI, Advanced operating systems, 30 heures eq TD, Master 1 informatique, Université Côte d’Azur.

International Master: Frédéric Mallet, Safety-Critical Systems, 32h.

Master: Frédéric Mallet, Software Engineering, 32h.

Master : Robert de Simone, Formal Methods for NoC-based design, 36 heures eq TD, M2 International Ubinet, Université Côte d’Azur.

M.A Peraldi-Frati teaches Web security (20h), Security of connected objects (20h), IoT Infrastructure deployment (20 H) and Large scale plateform for IoT (20h) in a licence cursus dedicated to Internet of Objects, Infrastructure and Applications.

Licence : Luigi Liquori, Peer-to-peer systems, 32 eq TD, Université Côte d’Azur.

Winter School on Theoretical Foundations of Computer Science, 4-9 February 2019, Georgia. Luigi Liquori. Peer-to-peer and reklated systems, International Black Sea University and Shota Rustaveli National Science Foundation of Georgia.

Master: Julien Deantoni, Finite State Machine, 54h eq TD, Polytech’Nice.

Master: Julien Deantoni, Multi Paradigm Programming in C++, 54h eq TD, Polytech’Nice.

Master: Julien Deantoni, Domain Specific Languages, 24h eq TD, Polytech’Nice.

Master: Julien Deantoni, Language Interpreter, 24h eq TD, Polytech’Nice.

10.2.2. Teaching Administration

- Sid Touati was the responsible of first year of computer science licentiate since 2011 till 2018.
- Sid Touati is a vice-director of the computer science department since 2017, in charge of the graduate students (licence).
- Frédéric Mallet is the coordinator of the International track of the Master of Computer Science since 2015.
- Frédéric Mallet is a member of the steering committee of the Graduate School DS4H (EUR DS4H).
- Master: Julien Deantoni, computer science internship management.

10.2.3. Supervision

- PhD in progress : Claude Stolze, A proof-functional type theory for intersection and union types, Université Côte d’Azur, end 2019, Luigi Liquori.
- PhD in progress : Carsten BRUNS, Performance analysis and optimisation of C++ applications, Université Côte d’Azur, 2021, Sid TOUATI.

- PhD in progress : Hui Zhao, Multiview System Integration for Cyber Physical Systems, Université Cote d'Azur, end 2019, Frédéric Mallet
- PhD in progress : Giovanni Liboni, Coordination of discrete (Cyber) Models, Université Cote d'Azur, end 2021, Frédéric Mallet, Julien DeAntoni

10.2.4. Juries

Robert de Simone was reviewer of the PhD thesis of Amaury Greillat (VERIMAG, Grenoble), and of the Habilitation thesis of Katell Morin-Allaury (TIMA, Grenoble).

M.A Peraldi-Frati : Examinator Thesis jury Slim Medimegh - CentraleSupélec University- Dec 2018.

Frédéric Mallet : Reviewer for the PhD thesis of NGuyen Van Hai - Université Paris Saclay - Central/Supélec, 27/09/2018

Frédéric Mallet : Reviewer for the PhD thesis of Martial Chabot - Université Grenoble Alpes - TIMA, 30/10/2018

PARKAS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Selection

9.1.1.1. Member of the Conference Program Committees

- T. Bourke served on the PC of the International Conference on Embedded Software (EMSOFT 2018).
- T. Bourke served on the PC for the Journées Francophones des Langages Applicatifs (JFLA 2018).
- T. Bourke served on the PC of the American Modelica Conference 2018.
- T. Bourke served on the PC of the Japanese Modelica Conference 2018.
- T. Bourke served on the PC of the International Workshop on Software and Compilers for Embedded Systems (SCOPES 2018).
- F. Zappa Nardelli will serve on the PC of OOPSLA 2019 (International Conference on Object-Oriented Programming, Systems, Languages & Applications).
- M. Pouzet served on the PC of the International Workshop on Software and Compilers for Embedded Systems (SCOPES 2018).
- M. Pouzet served on the PC of the International Conference on Embedded Software (EMSOFT 2018).
- M. Pouzet served on the PC of the International Conference on Principles and Practice of Declarative Programming (PPDP 2018).
- M. Pouzet served on the PC of the International Forum on specification & Design Languages (FDL 2018).

9.1.1.2. Reviewer

- T. Bourke reviewed for the International Joint Conference on Automated Reasoning (IJCAR 2018)
- T. Bourke reviewed for the International Conference on Interactive Theorem Proving (ITP 2018)
- T. Bourke reviewed for the International Symposium on Principles and Practice of Declarative Programming (PPDP 2018)

9.1.2. Journal

9.1.2.1. Reviewer - Reviewing Activities

- T. Bourke was a reviewer for Science of Computer Programming.

9.1.3. Invited Talks

- T. Bourke was invited to present a seminar at the Collège de France in January 2018: *La vérification formelle d'un compilateur Lustre*.
- T. Bourke was invited to present an LSV Seminar (Laboratoire Spécification et Vérification) at the ENS Cachan in January 2018: *Compiling a Synchronous Language with Timers for Simulation*
- T. Bourke was invited to present to the Société Informatique de France doctoral seminar at the École normale supérieure in June 2018: *10 lignes de logique pour 1 ligne de code (correct)*
- F. Zappa Nardelli was invited to present to the DeepSpec Workshop in July 2018 on *Debugging Debug Information*.

- T. Bourke and M. Pouzet participated by invitation in the Shonan Meeting 136 on *Functional Stream Libraries and Fusion: What's next?*, in Japan in October 2018.
- M. Pouzet was invited to give a lecture at the International summer school at Marktoberdorf, in July 2018.

9.1.4. Research Administration

- F. Zappa Nardelli will chair the part-time assistant professor recruitment committee at École Polytechinque.

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

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

Master: T. Bourke participated in reviewing the L3 and M1 internships of students at the ENS, France.

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

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

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

9.2.2. Supervision

PhD in progress : Lélio Brun, 3rd year, supervised by T. Bourke and M. Pouzet.

PhD in progress : Chandan Reddy, 3rd year, supervised by A. Cohen.

PhD : Jie Zhao, 3rd year, supervised by A. Cohen, defended in December 2018.

PhD in progress : Basile Clément, 1st year, supervised by F. Zappa Nardelli and A. Cohen.

9.2.3. Juries

- Francesco Zappa Nardelli was jury member of the PhD thesis of Francois Ginraud, Grenoble, Jan 2018.
- T. Bourke was an examiner for the thesis of Jiangchao LIU at the École normale supérieure in February 2018.
- T. Bourke was an examiner for the thesis of Hai NGUYEN VAN at the Université Paris-Sud in September 2018.
- T. Bourke was an examiner for the thesis of Narjes JOMAA at the Université de Lille in December 2018.
- F. Zappa Nardelli was an examiner for the thesis of Jie Zhao at the École normale supérieure in December 2018.

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

- F. Zappa Nardelli is member of the CES of Inria.

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).
- Jean-Bernard Stefani is the current chair of the steering committee of the IFIP FORTE international conference series, a member of the steering committee of the IFIP DISCOTEC conference series, and the current chair of the IFIP Working Group 6.1.

9.1.1.2. Member of the Organizing Committees

- Sophie Quinton was the co-organizer of a Dagstuhl seminar entitled “The Logical Execution Time Paradigm: New Perspectives for Multicore Systems”. https://www.dagstuhl.de/18092

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Alain Girault served in the program committees of the Symposium on Industrial Embedded Systems (SIES’18), the Forum on specification and Design Languages (FDL’18), and the Conference on Applications of Concurrency to System Design (ACSD’18).
- Gregor Gössler served in the program committees of the 18th International Workshop on Automated Verification of Critical Systems (AVOCS 2018) and the 3rd international Workshop on Formal Reasoning about Causation, Responsibility, and Explanations in Science and Technology (CREST 2018).
- Sophie Quinton served in the program committees of the 30th Euromicro Conference on Real-Time Systems (ECRTS’18), the 9th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems (WATERS’18), the 39th IEEE Real-Time Systems Symposium (RTSS’18) and the 26th International Conference on Real-Time Networks and Systems (RTNS’18).

9.1.2.2. Reviewer

- Alain Girault reviewed papers for the ECRTS’18 conference.

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 J. of Transportation Technologies (JTT) and IEEE Trans. Dependable and Secure Computing (TDSC).
- Gregor Gössler reviewed articles for IEEE Transactions on Automatic Control (TAC) and ACM Transactions on Embedded Computing Systems (TECS).
- Sophie Quinton reviewed an article for ACM Trans. on Embedded Computing Systems (TECS).

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.
- Xavier Nicollin is member of the committee for computing resources users ("Comité des Utilisateurs des Moyens Informatiques") of the Inria Grenoble – Rhône-Alpes research center.
- Jean-Bernard Stefani is head of science (délégué scientifique) of the Inria Grenoble – Rhône-Alpes research center and a member 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

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 (2017-2018), 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

Master: Jean-Bernard Stefani, Formal Aspects of Component Software, 9h, 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 SIF in progress: T. Mari, “From diagnosis to causal analysis”, U. Rennes, since November 2018, co-supervised by Gregor Gössler and Louise Travé-Massuyès (LAAS).
- PFE: Clément Arvis, “Génération automatique de musique”, Grenoble INP/Ensimag, September 2018, supervized by Sophie Quinton.

9.2.3. Juries

- Alain Girault was referee for the PhD thesis of Colin Vidal, Université Côte d’Azur, and for the PhD thesis of Julien Hascoet, INSA Rennes. He was also vice-president of the Inria Senior Researcher jury (DR2) and of the Inria Junior Researcher national jury (CRCN).
- Gregor Gössler was examiner for the PhD jury of Vincent Wang (U. Pennsylvania).
- Jean-Bernard Stefani was examiner for the Habilitation (HDR) jury of Thomas Ledoux (U. Nantes).
- Sophie Quinton was member of the CRCN jury in Rennes.

9.3. Popularization

9.3.1. Interventions

Sophie Quinton gave a keynote at the MathC2+ event organized by Inria, entitled “Faire des preuves par ordinateur : Pourquoi et comment ?” (Computer-assisted proofs: Why and how?).

TEA Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

Jean-Pierre Talpin served as Finance Chair and Local Organizer of the 16th J16th ACM-IEEE conference on methods and models for system design in Beijing, China (http://memocode.irisa.fr/2018) and its 1st embedded workshop on formal methods in China's industry.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Jean-Pierre Talpin served the program committee of:

- LCTES'18, 21th. ACM SIGPLAN-SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems
- SAC'19, 34rd. ACM SIGAPP Symposium on Applied Computing
- SCOPES'18, 21th. International Workshop on Software and Compilers for Embedded Systems

10.1.2.2. Reviewer

Thierry Gautier reviewed articles for *IEEE Access* and *Science of Computer Programming*.

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. Reviewer - Reviewing Activities

Thierry Gautier reviewed articles for *IEEE Access* and *Science of Computer Programming*.

10.1.4. Invited Talks

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

Thierry Gautier and Albert Benveniste gave a seminar on "The Signal synchronous language: the principles beyond the language and how to exploit and extend them", in March 2018 at the Collège de France, in Gérard Berry's 2017-2018 lecture course (https://www.college-de-france.fr/site/gerard-berry/seminar-2018-03-07-17h30.htm).

10.1.5. Expertise

Jean-Pierre Talpin served as vice-president of CES 25 (Computer Science Evaluation Committee) of ANR.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Jean-Pierre Talpin gave a seminar at Beihang Science Park on June 11th , at ISCAS on May 2nd and on June 14th, and at Beida (PKU) on December 7th. Jean-Pierre Talpin gave an introductory course on model-checking at Nankai University, May 7-8th.

10.2.2. Supervision

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

10.2.3. Juries

Jean-Pierre Talpin served as reviewer at the HDR Thesis defense of Katell Morin, entitled “Assertions and hardware design”, which took place at TIMA, Grenoble, on November 15.

Jean-Pierre Talpin served as reviewer at the PhD Thesis defense of Guillaume Plassan, entitled “Conclusive formal verification of clock domain crossing properties”, which took place at TIMA, Grenoble, on March 28.

ANTIQUE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

- Jérôme Feret is a guest member of the Steering Committee of the Conference on Computational Methods in Systems Biology (CMSB).
- Jérôme Feret is a member of the Steering Committee of the Workshop on Static Analysis and Systems Biology (SASB).
- Xavier Rival organized the 60th meeting of the IFIP Working Group 2.4 held in Dijon, in July 2018.
- Xavier Rival is a member of the Steering Committee of the Static Analysis Symposium (SAS).
- Xavier Rival is a member of the Steering Committee of the Workshop on Tools for Automatic Program Analysis (TAPAS).

8.1.2. Scientific Events Selection

8.1.2.1. Chair of Conference Program Committees

- Xavier Rival served as Chair of the Artifact Evaluation Committee of SAS 2018 (Static Analysis Symposium).

8.1.2.2. Member of the Conference Program Committees

- Jérôme Feret served as a Member of the Program Committee of LICS 2018 (Logic in Computer Science).
- Jérôme Feret served as a Member of the Program Committee of VEMDP 2018 (Verification of Engineered Molecular Devices and Programs).
- Jérôme Feret served as a Member of the Program Committee of SASB 2018 (Static Analysis and Systems Biology Workshop).
- Jérôme Feret served as a Member of the Program Committee of SAS 2018 (Static Analysis Symposium).
- Jérôme Feret served as a Member of the Program Committee of CMSB 2018 (Computational Methods in Systems Biology).
- Jérôme Feret served as a Member of the Program Committee of VMCAI 2019 (Verification, Model Checking, and Abstract Interpretation)
- Jérôme Feret is serving as a Member of the Program Committee of CIBCB 2019 (Computational Intelligence in Bioinformatics and Computational Biology).
- érôme Feret is serving as a Member of the Program Committee of HSB 2019 (Hybrid Systems and Biology).
- Jérôme Feret is serving as a Member of the Program Committee of CMSB 2019 (Computational Methods in Systems Biology).
- Xavier Rival served as a Member of the Program Committee of SAS 2018 (Static Analysis Symposium).
- Xavier Rival served as a Member of the Program Committee of Web Design, Analysis, Programming and Implementation of the WWW'18 Conference.

- Xavier Rival served as a Member of the Extended Review Committee of PLDI 2018 (Programming Languages Design and Implementation).
- Xavier Rival served as a Member of the Program Committee of APLAS 2018 (Asian Programming Languages And Systems Symposium).
- Xavier Rival is serving as a Member of the Committee of POPL 2020 (Principles of Programming Languages).
- Cezara Drăgoi served as a member of the Program Committee of Computer Aided Verification CAV'18.
- Cezara Drăgoi served as a member of the Program Committee of VMCAI 2019 (Verification, Model Checking, and Abstract Interpretation).
- Cezara Drăgoi served as a member of the Program Committee of NETYS 2018.

8.1.2.3. Reviewer

- Jérôme Feret served as Reviewer for ARSBM 2018 (Automated Reasoning for Systems Biology and Medicine).

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

- Jérôme Feret serves as a Member of the Editorial Board of the Frontiers in Genetics journal and the Open Journal of Modeling and Simulation.
- Jérôme 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 2019.
- Jérôme Feret serves as co-Editor of an Issue of the IEEE/ACM Transactions on Computational Biology and Bioinformatics, that is composed of papers from CMSB 2017, 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 appeared in 2018.

8.1.3.2. Reviewer - Reviewing Activities

- Jérôme Feret served as a Reviewer for NACO (Natural Computing).
- Jérôme Feret served as a Reviewer for ACS Synthetic Biology.
- Jérôme Feret served as a Reviewer for TCS (Theoretical Computer Sciences).
- Jérôme Feret served as a Reviewer for TCBB (IEEE/ACM Transactions on Computational Biology and Bioinformatics).
- Jérôme Feret served as a Reviewer for IEEE Transactions on Reliability.
- 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).

8.1.4. Invited Talks

- Cezara Drăgoi was invited to give a talk at the workshop on Verification of Distributed Systems, Essaouira, Morocco, 2018.
- Cezara Drăgoi was invited to give a talk at the Dagstuhl workshop no 18211 on Formal Methods and Fault-Tolerant Distributed Computing: Forging an Alliance.

8.1.5. Leadership within the Scientific Community

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

8.1.6. Scientific Expertise

- Cezara Drăgoi has participated to the recruitment committee for an assistant professor in the Department of Computer Science of École normale supérieure 2018.
- Jérôme Feret served as a external Reviewer for research program PRIM 2017 (funded by MIUR, the Italian Ministry for Education, University and Research).
- Jérôme Feret has participated to the recruitment committee for an assistant professor in Paris-Diderot University 2018.
- Xavier Rival chaired the Hiring Committee for an Assistant Professor position (Tenure track position, Gaspard Monge Chair) at École Polytechnique in 2018.

8.1.7. Research Administration

- Jérôme Feret and Xavier Rival are members of the Laboratory Council of DIENS.
- Jérôme Feret is member of PhD Review Committee (CSD) of Inria Paris.
- Jérôme Feret is deputy head of study of the Department of Computer Science of École normale supérieure.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence:

- Marc Chevalier, Mathematics, 40h, L1, FDV Bachelor program (Frontiers in Life Sciences (FdV)), Université Paris-Descartes, France.
- Jérôme Feret and Xavier Rival (lectures), and Marc Chevalier (tutorials), “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.

Master:

- Xavier Rival, “Introduction to Static Analysis”, 24h, Internet of Things Master (retraining curriculum, EXED), France.
- Xavier Rival, “Protocol Safety and Verification”, 12h, M2, Advanced Communication Networks Master, France.
- Cezara Drăgoi, Jérôme 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 Jérôme Feret (with Jean Krivine), Computational Biology, 28h, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.

Doctorat:

- Jérôme Feret, “Intrinsic Coarse-Graining of Models of Signalling pathways", 1h30, aDVANCES IN SYSTEMS AND SYNTHETIC BIOLOGY Modelling Complex Biological Systems in the Context of Genomics Thematic Research School, March 2018, Évry, France.

8.2.2. Supervision

- PhD in progress: Marc Chevalier, Static analysis of Security Properties in Critical Embedded Software. started in 2017 and supervised by Jérôme 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: Olivier Nicole, Verification of micro-kernels, started in 2018 and supervised by Xavier Rival and Matthieu Lemerre (CEA)
- PhD defended: Huisong Li, Disjunctive Shape Abstraction for Shared Data-Structures, started in 2014 and supervised by Xavier Rival
- PhD defended: Jiangchao Liu, Static Analysis for Numeric and Structural Properties of Array Contents, started in 2014 and supervised by Xavier Rival

8.2.3. Juries

- 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).

8.3. Popularization

8.3.1. Internal or external Inria responsibilities

- Xavier Rival is member of the “Bureau du comité des projets” since October 2018.
- Xavier Rival is Chair of the Hiring Committee for Inria researchers at the center of Paris (CRCN) for 2019.

CELTIQUE Project-Team

7. Dissemination

7.1. Promoting Scientific Activities

7.1.1. Scientific Events Organisation

7.1.1.1. Member of the Organizing Committees

- Formal Methods meet JavaScript Workshop 2018, organizer: Alan Schmitt

7.1.2. Scientific Events Selection

7.1.2.1. Chair of Conference Program Committees

- AVoCS 2018 (International workshop on automated verification of critical systems), FLOC workshop, Oxford (co-chair) : David Pichardie

7.1.2.2. Member of the Conference Program Committees

- CC 2018 (International Conference on Compiler Construction) : David Pichardie
- CPP 2018 (ACM SIGPLAN Conference on Certified Programs and Proofs) : Sandrine Blazy
- ITP 2018 (International Conference on Interactive Theorem Proving) : Delphine Demange
- Euro S&P 2018 (IEEE European Symposium on Security and Privacy) : Sandrine Blazy
- ICFP 2018 (ACM SIGPLAN International Conference on Functional Programming) : Sandrine Blazy
- LOPSTR 2018 (Symposium on Logic-Based Program Synthesis and Transformation) : Sandrine Blazy
- SAS 2018 artefact evaluation committee : Frédéric Besson
- ProWeb 2018: Alan Schmitt

7.1.3. Journal

7.1.3.1. Reviewer - Reviewing Activities

- Discrete Mathematics & Theoretical Computer: Alan Schmitt
- Theoretical Computer Science: Alan Schmitt
- Theoretical Informatics and Applications: Alan Schmitt

7.1.4. Invited Talks

- F. Besson gave a talk at the Dagstuhl Seminar 18201 "Secure Compilation".
- T. Genet gave an invited talk at the ETAPS “Workshop on Rewriting Logic and Applications” in Thessaloniki [12].

7.1.5. Leadership within the Scientific Community

- Sandrine Blazy coordinated of the LTP (Languages, Types, Proofs) group of the French GDR GPL (until October 2018).
- Thomas Jensen is head of the research axis “Security and Privacy” at the Labex CominLabs.
- Sandrine Blazy and Thomas Jensen are member of the Steering Committee of Static Analysis Symposium (SAS).

7.1.6. Scientific Expertise

- Sandrine Blazy: expertise of an ERC Advanced Grant research proposal

- David Pichardie: expertise of two ERC Advanced Grant research proposals
- Sandrine Blazy and David Pichardie : members of the HCERES evaluation committee of the LSV laboratory in December 2018
- David Pichardie: expertise of 1 ANR project
- David Pichardie, jury member for the selection of a Maître de Conférences at ENSEEIHT (Toulouse), May 2018
- Thomas Jensen: expertise of an ERC Consolidator Grant research proposal
- Alan Schmitt: expertise of a Innovational Research Incentives Scheme Veni research proposal
- Sandrine Blazy is member of IFIP WG 2.11 on program generation and of IFIP WG 1.9/2.15 on verified software

7.1.7. Research Administration

- Sandrine Blazy is member of Section 6 of the national committee for scientific research CoNRS.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence : Sandrine Blazy, Programmation de confiance, 81h, L3, Université Rennes 1, France

Licence : David Cachera, Initiation to Pedagogy and Mediation, 11h, L3, ENS Rennes, France

Licence : David Cachera, Algorithmics, 20h, L3, ENS 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 : Thomas Genet, Spécialité Informatique 1 - Algorithmique et Complexité Expérimentale, 47h, L1, Université Rennes 1, France

Licence : Thomas Genet, Initiation au génie logiciel, 67h, L2, Université Rennes 1, France

Licence : Thomas Jensen, Programmation de confiance, 20h, L3, Université Rennes 1, France

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

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

Licence : Alan Schmitt, Programmation de Confiance, 28h, L3, Université Rennes 1, France France

Master : Sandrine Blazy, Static analysis, 30h, M1, Université Rennes 1, France

Master : Sandrine Blazy, Mechanized Semantics, 30h, M2, Université Rennes 1, France

Master : Sandrine Blazy, Software vulnerabilities, 26h, M2, Université Rennes 1, France

Master : David Cachera, Semantics of Programming Languages, 28h, M1, Université Rennes 1, France

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

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

Master : Thomas Genet, Analyse et conception formelle, 65h, M1, Université Rennes 1, France

Master : David Pichardie, Static analysis, 30h, M1, Université Rennes 1, France

Master : David Pichardie, Preparation of Agregation exam, 70h, M2, ENS Rennes, France

Master : Thomas Jensen, Software Security, 21h, M2, Université Rennes 1, France.

7.2.2. Supervision

PhD : Yon Fernandez De Retana, Toward verified compilation of Sea of Nodes : semantic properties and reasoning, Université Rennes 1, defended 5 July 2018, Delphine Demange and David Pichardie

PhD : Alix Trieu, Verifying constant-time implementations in a verified compilation toolchain, Université Rennes 1, defended 4 December 2018, Sandrine Blazy and David Pichardie

PhD: Gurvan Cabon, Analyse non locale certifiée en JavaScript grâce à une sémantique annotée, Université Rennes 1, defended 14 December 2018, Alan Schmitt

PhD in progress : Timothée Haudebourg, Verification of Higher-Order Functional Programs using Tree Automata, September 2017, Thomas Genet and Thomas Jensen

PhD in progress : Rémi Hutin, A C compiler ensuring security properties, September 2018, Sandrine Blazy and David Pichardie

7.2.3. Juries

- Sandrine Blazy, jury member for the selection of CNRS CR and DR (researchers) candidates, February and March 2018, CNRS, Paris, France.
- Sandrine Blazy, jury member for the promotion to a senior lecturer position at the University of Kent, May 2018, Canterbury, Great Britain
- Sandrine Blazy, jury member (reviewer) for the PhD defense of Martin Clochard, March 2018, Paris-Sud University
- Sandrine Blazy, jury member for the PhD defense of Huisong Li, March 2018, ENS, Paris
- Sandrine Blazy, jury member for the HDR defense of Aurélie Hurault, July 2018, Université de Toulouse
- Sandrine Blazy, jury member of the GDR GPL PhD award committee.
- Thomas Jensen, president of jury for the PhD defense of Yon Fernandez de Retana, July 2018, University of Rennes 1.
- Alan Schmitt, jury member (reviewer) for the PhD defense of Guillaume Claret, September 2018, Université Sorbonne Paris Cité
- Sandrine Blazy, jury member for the PhD defense of Rabab Bouziane, December 2018, Université Rennes 1
- David Pichardie, jury member (reviewer) for the PhD defense of Jiangchao Liu, February 2018, Paris Sciences et Lettres Research University
- David Pichardie, jury member (reviewer) for the PhD defense of Thibaut Girka, July 2018, Université Paris-Diderot
- David Pichardie, jury member (reviewer) for the PhD defense of Jean-Christophe Léchenet, July 2018, Université Paris-Saclay
- David Pichardie, jury member (reviewer) for the PhD defense of Sigurd Schneider, November 2018, Saarland University, Germany
- David Pichardie, jury member (reviewer) for the PhD defense of Narjes Jomaa, December 2018, Université de Lille
- Frédéric Besson, member of hiring committee for a Maître de Conférence position, Spring 2018, ENSIMAG

7.3. Popularization

7.3.1. Interventions

- Thomas Genet gave a talk “Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths.” in high schools close to Rennes. 2018.
- David Cachera contributed to the animation of “École Médiation scientifique en informatique ”, Société Informatique de France, June 2018.

CONVECS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Member of the Organizing Committees

- H. Garavel is a member of the model board [0] of MCC (*Model Checking Contest*). In 2018, 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'2018 have been published online [51].
- 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 21 models, one of which (a Transport Layer Security protocol) was deposited in 2018 by CONVECS.
- G. Salaün is member of the steering committee of the ACM SAC-SVT (*Symposium of Applied Computing – Software Verification and Testing Track*) conference series since 2018.
- 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. Salaün was co-chair of ACM SAC-SOAP'2018 (*33rd ACM Symposium of Applied Computing – Service-Oriented Architectures and Programming Track*), Pau, France, April 9–13, 2018.
- G. Salaün was workshops co-chair at STAF'2018 (*Software Technologies: Applications and Foundations*), Toulouse, France, June 25-29, 2018.
- W. Serwe was co-chair of MARS'2018 (*3rd Workshop on Models for Formal Analysis of Real Systems*) affiliated with ETAPS'2018 (*European Joint Conferences on Theory and Practice of Software*), Thessaloniki, Greece, April 20, 2018.

9.1.2.2. Member of the Conference Program Committees

- H. Garavel was program committee member of FVPS'2018 (*International Workshop on Formal Verification of Physical Systems*), Hagenberg, Austria, August 17, 2018.
- F. Lang was program committee member of SPIN'2018 (*25th International SPIN Symposium on Model Checking of Software*), Málaga, Spain, June 20–22, 2018.
- R. Mateescu was program committee member of ICTSS'2018 (*30th IFIP International Conference on Testing Software and Systems*), Cádiz, Spain, October 1–3, 2018.
- R. Mateescu was program committee member of FMICS'2018 (*23rd International Conference on Formal Methods for Industrial Critical Systems*), Maynooth, Ireland, September 3–4, 2018.
- G. Salaün was program committee member of CAL'2018 (*11ème Conférence francophone sur les Architectures Logicielles*), Grenoble, France, June 14–15, 2018.
- G. Salaün was program committee member of COMPSAC'2018 (*IEEE International Conference on Computers, Software, and Applications*), Tokyo, Japan, July 23–27, 2018.

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

- G. Salaün was program committee member of DATAMOD’2018 (*7th International Symposium “From Data to Models and Back”*), Toulouse, France, June 25–26, 2018.
- G. Salaün was program committee member of FACS’2018 (*15th International Conference on Formal Aspects of Component Software*), Pohang, Korea, October 10–12, 2018.
- G. Salaün was program committee member of FOCLASA’2018 (*16th International Workshop on Foundations of Coordination Languages and Self-Adaptative Systems*), Toulouse, France, June 26, 2018.
- G. Salaün was program committee member of HPCS-4PAD’2018 (*5th International Symposium on Formal Approaches to Parallel and Distributed Systems*), Orléans, France, July 16–20, 2018.
- G. Salaün was program committee member of SEFM’2018 (*16th International Conference on Software Engineering and Formal Methods*), Toulouse, France, June 27–29, 2018.
- G. Salaün was program committee member of SAC-SVT’2018 (*33rd ACM Symposium on Applied Computing - Software Verification and Testing Track*), Pau, France, April 9–13, 2018.

9.1.2.3. Reviewer

- G. Barbon was a reviewer for COMPSAC’2018, DATAMOD’2018, and SEFM’2018.
- F. Lang was a reviewer for FoSSaCS’2018 (*21st International Conference on Foundations of Software Science and Computation Structures*).
- A. Muroor Nadumane was a reviewer for COMPSAC’2018, FACS’2018, FOCLASA’2018, SAC-SVT’2018, and SEFM’2018.
- U. Ozeer was a reviewer for COMPSAC’2018.
- R. Mateescu and W. Serwe were reviewers for the Festschrift in honor of Bernhard Steffen.

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 FAoC (*Formal Aspects of Computing*) and ToCL (*ACM Transactions on Computational Logic*).
- R. Mateescu was a reviewer for STTT, ToCL, and TOR (*IEEE Transactions on Reliability*).
- A. Muroor Nadumane was a reviewer for STTT.
- G. Salaün was a reviewer for FAoC, JCC (*Journal of Computer and Communications*), JLAMP (*Journal of Logical and Algebraic Methods in Programming*), SCP (*Science of Computer Programming*), TSE (*IEEE Transactions on Software Engineering*), TSI (*Technique et Science Informatiques*).

9.1.4. Software Dissemination and Internet Visibility

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

In 2018, the main facts are the following:

- We prepared and distributed twelve successive versions (2018-a to 2018-l) of CADP.
- We were requested to grant CADP licenses for 381 different computers in the world.

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

By the end of December 2018, the CADP forum [0], opened in 2007 for discussions regarding the CADP toolbox, had over 426 registered users and over 1847 messages had been exchanged.

[0] http://convecs.inria.fr

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

Also, for the 2018 edition of the Model Checking Contest, 4 families of models generated using CADP (totalling 101 Nested-Unit Petri Nets) were provided.

We contributed to Wikipedia as follows:

- We created a new page about the Message Authenticator Algorithm (https://en.wikipedia.org/wiki/Message_Authenticator_Algorithm)
- We added the three last paragraphs of the section about constructing integer numbers (https://en.wikipedia.org/wiki/Integer#Construction)

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 RichTest Tool for Message-Passing Concurrent Programs [33]
- The REFINER Tool for Verifying Behavioural Model-to-Model Transformations [63]
- The ALVIS Tool for Modelling and Verification of Real-Time Systems [60]
- The COSTO Tool for Component-Based Software [30]
- The IDCM Tool for Analyzing UML Architectures [52]
- The OCARINA Tool and its Extension AADL2LNT for Analysing AADL Descriptions [58]
- The aZiZa Tool for Heterogeneous Behavioural Models [31]
- The Papyrus-RT Tool for Model-driven Engineering with UML-RT [62]
- Formal Analysis of Distributed Reactive Applications [35], [34]

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

- Formal Modelling and Verification of an Automatic Train Supervision System [56], [57]
- Verification of Highly-Optimized Concurrent Data Structures [61]
- Detection of Data Breaches in Banking Transaction Processes [54]
- Verification of Visibility-Based Properties on Multiple Moving Robots [59]
- Experimental Analysis of Compositional State Space Generation Strategies [64]
- Product-Line for Families of Program Translators [32]

9.1.5. Invited Talks

- H. Garavel participated in the workshop "*Safety of Future Systems: Science meets Industry*" organized by the Lorentz Center (Leiden, The Netherlands) on April 9–13, 2018. He gave a lecture entitled "*Concurrency Theory Meets IoT*".
- H. Garavel gave an invited talk entitled "*Benchmarking Implementations of Term Rewriting and Pattern Matching in Algebraic, Functional, and Object-Oriented Languages - The 4th Rewrite Engines Competition*" at WRLA'2018 (*12th International Workshop on Rewriting Logic and its Applications*), Thessaloniki, Greece, April 14–15, 2018.
- L. Marsso gave a talk and presented a poster entitled "*Automated Test Generation for GALS Systems*" on March 8, 2018 at the 2nd year PhD LIG Day.
- L. Marsso gave a talk entitled "*Generation with CADP of Relevant Scenarios for Testing Autonomous Cars*" at the seminar of the group TransForm (*Méthodes formelles pour les systèmes de transport*) held in Villeneuve d'Ascq on November 22, 2018.
- L. Marsso gave a talk entitled "*Automated Test Generation for GALS Systems*" at the Scientific day of ARC 6 held in Lyon on November 29, 2018.
- R. Mateescu participated to the Kobe-Grenoble workshop organized by UGA in Grenoble on February 26–27, 2018. He gave a talk entitled "*Rigorous Design of PLC Networks using Formal Methods*" on February 26.

- A. Muroor Nadumane gave a talk entitled "*Building Reliable IoT Application and Beyond*" at the Inria-Nokia Bell Labs meeting held in Paris on November 27, 2018.
- U. Ozeer gave a talk and presented a poster entitled "*Autonomous Resilience of Distributed IoT Applications in a Fog Environment*" on March 8, 2018 at the 2nd year PhD LIG Day.
- U. Ozeer gave a talk entitled "*Autonomous Resilience of Distributed IoT Applications in a Fog Environment*" at the seminar on IoT research projects held at Orange Labs, Meylan, on March 29–30, 2018.
- U. Ozeer presented a poster entitled "*Autonomous Resilience of Distributed IoT Applications in a Fog Environment*" at the LIG seminar "*Regards sur le futur de l'informatique*" held in Grenoble on April 6, 2018.
- U. Ozeer gave a talk entitled "*Resilience of Distributed IoT Applications in a Dynamic Fog Environment*" at the IO Labs seminar held in Paris on October 30–31, 2018.
- G. Salaün gave a keynote talk entitled "*Safe Composition of Software Services*" at DATAMOD'2018, Toulouse, France, on June 26, 2018.

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 (*Pervasive Computing Systems*) 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 2018, we carried out the following teaching activities:

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 2018.

F. Lang and R. Mateescu gave a lecture on "*Modeling and Analysis of Concurrent Systems: Models and Languages for Model Checking*" (27 hours "*équivalent TD*") to third year students of ENSIMAG and second year students of the MOSIG (*Master of Science in Informatics at Grenoble*).

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.

F. Lang and W. Serwe provided a 6-hour training about the CADP toolbox to Eric Jenn, Nicolas Hili, and Sun Wei Tsun (IRT Saint-Exupéry, Toulouse, France) on June 28, 2018.

L. Marsso gave a course on "*Algorithms and Web Programming*" (64 hours "*équivalent TD*") at the department MMI of IUT1 (UGA).

A. Muroor Nadumane gave a course on "*Object Oriented Programming*" (42 hours "*équivalent TD*") at the department MMI of IUT1 (UGA).

G. Salaün taught about 230 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: 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, L. Letondeur, G. Salaün, F.-G. Ottogalli, and J.-M. Vincent

9.2.3. Juries

- G. Salaün was PhD committee member for Gustavo García Pascual's PhD thesis, entitled "*Optimizing Mobile Applications by Exploiting Variability Models at Runtime*", defended at University of Málaga (Spain) on December 18, 2018.

DEDUCTEAM Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organization

Guillaume Burel has been local organizer of the scientific days of the CNRS GDR GPL working groups LTP and MTV2.

9.1.2. Scientific Events Selection

Frédéric Blanqui has been PC chair of the 13th International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice (LFMTP'18) with Giselle Reis.

Frédéric Blanqui is Workshop Chair of LICS and member of the Steering Committee of LICS.

Frédéric Blanqui is member of the Steering Committee of the International School on Rewriting (ISR) of the WG 1.6 of the International Federation for Information Processing.

Gilles Dowek has been a PC member of TYPES 2018.

Guillaume Burel has been PC member of the 30th Journées Francophones des Langages Applicatifs.

Guillaume Burel has reviewed a submission for the International Conference on Principles and Practice of Constraint Programming (CP). Guillaume Genestier reviewed submissions to the conferences Logic in Computer Science (LICS), Principles and Practice of Declarative Programming (PPDP) and European Symposium on Programming (ESOP).

9.1.3. Journals

Gilles Dowek is an editor of TCS-C.

Frédéric Blanqui has reviewed a paper for Mathematical Structures in Computer Science (MSCS). Guillaume Burel has reviewed papers for the Computer Journal and Logical Methods in Computer Science (LMCS). Rodolphe Lepigre has reviewed a paper for International Conference on Foundations of Software Science and Computation Structures (FoSSaCS). Rodolphe Lepigre has reviewed a paper for the journal ACM Transactions on Programming Languages and Systems (TOPLAS). Franck Slama has reviewed a paper for the Journal of Functional Programming.

9.1.4. Invited Talks

- Rodolphe Lepigre gave an invited talk entitled "The PML Language: Realizability at the Service of Program Proofs" at the Realizability Workshop (12-13 June 2018) in Luminy.
- Rodolphe Lepigre gave an invited talk entitled "An Overview of the PML_2 Language: Realizability, Subtyping and Cyclic Proofs" at LRI, for the starting days of the new Scalp working group of GDR IM. This is a presentation of his paper [32].
- Gilles Dowek has given an invited talk at NFM (Nasa Formal Methods).
- Jean-Pierre Jouannaud has given an invited talk at the workshop "Rewriting Techniques for Program Transformation and Evaluation" at FLoC, on July 8, 2018.

9.1.5. Seminars

- Gilles Dowek has participated to the meeting "From Information to Cells" organized by Hélène Kirchner and Antoine Danchin. He has given a talk at the National Institute of Aerospace.
- Gilles Dowek has co-organized a seminar on Logic and Philosophy at the CNFHPST.

- Guillaume Burel has presented a talk entitled “Bridging holes on DEDUKTI proofs, an overview” at the scientific day of the Digicosme working group UPSCaLe.
- Bruno Barras has given a talk entitled “An analysis of bindlib” at the UPSCaLe meeting (June’18) held in Palaiseau.
- Mohamed Yacine EL HADDAD has presented his work at internal laboratory seminar of LSV (June’18) and SAMOVAR (November’18).
- Gaspard Férey has presented his work at internal laboratory seminar of LSV (June’18).
- Guillaume Genestier has presented his work at the internal laboratory seminar of Centre de Recherche en Informatique of Mines ParisTech (February’18) and LSV (June’18) and presented DEDUKTI at the doctoral seminar of La Société Informatique de France (June’18). He presented [16] in the WorkShop on Termination (WST) at Oxford (July’18).
- Rodolphe Lepigre has presented his work on "Termination checking using well-founded typing derivations" at a Deducteam seminar in September 2018.
- Rodolphe Lepigre has given a talk entitled “The PML_2 Language, Integrated Program Verification in ML” at the Max Planck Institute for Software Systems in Saarbrücken, in November 2018.
- Franck Slama has presented some previous work at an internal laboratory seminar of LSV in December 2017.
- François Thiré has presented his work on interoperability at the UPSCaLe seminar on March 2018, then he presented his paper [15] at the LFMT Workshop at Oxford (July’17).
- Aristomenis Papadopoulos has presented the work he did during his summer internship at a Deducteam seminar in September 2018.

9.1.6. Leadership within the scientific community

Gilles Dowek is president of the scientific board of the Socitété informatique de France.

He is a member of the Ethic council CERNA.

He is a member of the Comité National Français d’Histoire et de Philosophie des Sciences et des techniques.

He is a member of the scientific board of La Main à la pâte.

He is a member of the scientific board of the Institut Villebon Charpak.

He is a member of the scientific board of the Maison des sciences de Lorraine.

He is the president of the Board of teacher school (ESPE) of the University of Lorraine.

He is a member of the scientific board of SystemX.

He is a member of the scientific board of the team Humanités numériques at the Collège des Bernardins.

Gilles Dowek and Jean-Pierre Jouannaud are honorary members of IFIP-WG1.6.

Jean-Pierre Jouannaud is a permanent member of the visiting committee of Academia Sinica, Taiwan.

9.1.7. Scientific Expertise

Frédéric Blanqui reviewed a project for the Netherlands Organization for Scientific Research (NWO).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master: Bruno Barras, proof assistants, 12h, M2, MPRI
- Master: Frédéric Blanqui, formal languages, 21h, M1, ENSIIE
- Master: Frédéric Blanqui, rewriting theory, 14h, M1, ENS Paris-Saclay

- Master: Frédéric Blanqui, λ-calculus and theories in first-order logic, 18h, M1/M2, ENS Paris-Saclay
- Master: Gilles Dowek has given a course at MPRI.
- Master: Gilles Dowek is in charge of the second year of Masters at the École normale de Paris Saclay.
- Master: Gilles Dowek has given a one week invited course at the University of Buenos Aires.
- Licence: Guillaume Genestier, logic tutorials, 45h, L3, ENS Paris-Saclay
- Licence: Guillaume Genestier, complexity remedial classes, 11h, L3, ENS Paris-Saclay
- Licence: Gaspard Férey, language theory, 44h, L3, EISTI
- Licence: François Thiré, (spring) logic project, 26h, L3 ENS Paris-Saclay
- Licence: François Thiré, (spring) Programmation 2 tutorials, 26h, L3 ENS Paris-Saclay
- Licence: François Thiré, (fall) Architectures and Systems tutorials, 36h, L3 ENS Paris-Saclay
- Frédéric Blanqui is co-director of the pole 4 of the doctoral school STIC of the University Paris-Saclay.
- Frédéric Blanqui is member of the committee of the doctoral school of the ENS Paris-Saclay.
- Frédéric Blanqui is in charge of following PhD students at LSV.

9.2.2. Supervision

- PhD Defended: Frédéric Gilbert, Gilles Dowek and Florent Kirchner,
- PhD in progress: Guillaume Bury, David Delahaye and Gilles Dowek,
- PhD in progress: Guillaume Genestier, termination in $\lambda\Pi$-calculus modulo theory, 01/10/17, Frédéric Blanqui and Olivier Hermant,
- PhD in progress: Mohamed Yacine El Haddad, using automated provers in proof assistants, 05/01/18, Frédéric Blanqui and Guillaume Burel,
- PhD in progress: Gaspard Férey, Associative-Commutative rewriting in the $\lambda\Pi$-calculus, 01/09/18, Gilles Dowek,
- PhD in progress: François Thiré, Design tools to make interoperability easier in DEDUKTI, 01/09/18, Gilles Dowek.

9.2.3. Juries

Gilles Dowek has been a member of the Jury of the PhD defence of Pierre Boutry. He has been an evaluator of the thesis of Thibault Gauthier. He has been a member of the Jury of the habilitation defence of Julien Signoles and of Alexei Grinbaum.

9.3. Popularization

9.3.1. Articles and contents

Gilles Dowek writes a monthly column in Pour la Science (12 issues) and has started a bi-monthly column in Le Monde (3 issues).

Gilles Dowek has given interviews to France Inter, Radio France Internationale, France Culture, Ouest France, Usbek et Rica, and Philosophie Magazine.

9.3.2. Education

Gilles Dowek has participated to meetings on scientific education in Switzerland, Belgium, and Côte d'Ivoire.

He has been heard by a committee of the the Éducation Nationale on pedagogical data and privacy.

He has given a talk on job mutations to mathematics inspectors.

9.3.3. Interventions

Gilles Dowek has given popular science talks in Toulouse, Antony, Issoudun, Rueil Malmaison, Saint Louis, Saint-Cloud, Rennes, Nancy, Paris, Nîmes, St Quentin en Yvelines, Montbéliard, Molaix, St Agrève, Rhodes, Marcoule, and Juvisy.

GALLINETTE Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

- N. Tabareau has co-organized (with Matthieu Sozeau) the Coq Workshop as part of FLoC 2018.
- A. Mahboubi has co-chaired (with Jeremy Avigad) the ITP 2018 conference, part of FLoC 2018.

8.1.1.2. Member of the Organizing Committees

- A. Mahboubi has co-organized (with Andrej Bauer, Martin Escardó and Peter Le Fanu Lumsdaine) the Dagsthul seminar 19341, Formalization of Mathematics in Type Theory.

8.1.2. Scientific Events Selection

8.1.2.1. Chair of Conference Program Committees

- A. Mahboubi has served in the FLoC 2018 Program Committee and Workshops Committee.

8.1.2.2. Member of the Conference Program Committees

- N. Tabareau has been a member of the program committee of FSCD'18 and ICFP'18 (External Review Committee).
- A. Mahboubi has been a member of the program committee of the CPP 2018 and CICM 2018 conferences, and of the TYPES 2018 and HOTT/UF 2018 workshops.

8.1.2.3. Reviewer

- N. Tabareau has served as an external reviewer for MFCS'18, WoLLIC'18.
- A. Mahboubi has served as external reviewer for the post-proceedings of TYPES 2017.

8.1.3. Journal

8.1.3.1. Member of the Editorial Boards

- A. Mahboubi is a member of the editorial board of the Journal of Automated Reasoning.
- A. Mahboubi is associate editor of the Progress in Computer Science and Applied Logic series.

8.1.3.2. Reviewer - Reviewing Activities

- A. Mahboubi has served as reviewer for the Journal of Automated Reasoning, and for the Annals of Mathematics and Artifical Intelligence.
- G. Munch-Maccagnoni has served as reviewer for the Journal of Automated Reasoning, and for Logical Methods in Computer Science.

8.1.4. Invited Talks

- A. Mahboubi has given an invited talk at the conference in honour of Thomas C. Hales on the occasion of his 60th birthday.
- A. Mahboubi has given an invited course at the Journées Nationales du Calcul Formel 2018.
- A. Mahboubi has given an invited course at the 19th Journées Louis Antoine.
- A. Mahboubi and G. Munch-Maccagnoni have given invited talks in the seminar organized by Xavier Leroy at the Collège de France in December.
- G. Munch-Maccagnoni has given an invited talk at the Journées Inaugurales du GT Scalp in November.

- G. Munch-Maccagnoni has given an invited talk at the seminar of the Celtique team in Rennes in October.
- G. Munch-Maccagnoni has given an invited talk at the seminar of the Gallium team in Paris in June.
- G. Munch-Maccagnoni has given an invited talk at the Logic and Semantics seminar at the University of Cambridge in June.

8.1.5. Leadership within the Scientific Community

- A. Mahboubi is a member of the scientific committee of the GdR Informatique-Mathématiques.
- A. Mahboubi is MC member for the COST Action CA15123 EUTypes, and a member of the core managment group of the project. She is leading the working group "Type-Theoretic Tools".

8.1.6. Research Administration

- A. Mahboubi has served in the Inria commitee examining the "Candidatures en détachements".
- A. Mahboubi has served as internal examiner in the jury of two "Maître de conférence" positions at Université de Nantes.
- A. Mahboubi has served in the jury of an assistant professor position in computer science at Stockholm University (Sweden).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Julien Cohen, Discrete Mathematics, 48h, L1 (IUT Informatique), IUT Nantes, France

Licence : Object oriented programming, 32h, L3 (Ingineering school), Polytech Nantes, France

Master : Functional programming, 18h, M1 (Ingineering school), Polytech Nantes, France

Master : Tools for softaware engineering (proof, test, code management), 20h, M1 (Ingineering school), Polytech Nantes, France

Licence : Rémi Douence, Object Oriented Programming Project, 45h, L1 (apprenticeship), IMT-Atlantique, Nantes, France

Licence : Rémi Douence, Object Oriented Design and Programming, 25h , L3 (engineers), IMT-Atlantique, Nantes, France

Licence : Hervé Grall, Object Oriented Design and Programming, 25h , L3 (engineers), IMT-Atlantique, Nantes, France

Licence : Rémi Douence, Data Structures and Algorithms, 20h , L2 (engineers), IMT-Atlantique, Nantes, France

Licence : Rémi Douence, GUI, 20h, L2 (engineers), IMT-Atlantique, Nantes, France

Licence, Master : Hervé Grall, Modularity and Typing, 40h, L3 and M1, IMT-Atlantique, Nantes, France

Licence : Guilhem Jaber, Computer Tools for Science, 36h, L1, Université de Nantes France

Licence : Guilhem Jaber, Computer Architecure, 36h, L3, Université de Nantes France

Master : Hervé Grall, Service-oriented Computing, 40h, M1 and M2, IMT-Atlantique, Nantes, France

Master : Rémi Douence, Functional Programming with Haskell, 20h, M1 (engineers), IMT-Atlantique, Nantes, France

Master : Rémi Douence, Functional Programming with Haskell, 20h, M1 (apprenticeship), IMT-Atlantique, Nantes, France

Master : Rémi Douence, Introduction to scientific research in computer science (Project: an Haskell interpreter in Java), 45h, M2 (apprenticeship), IMT-Atlantique, Nantes, France

Master : Hervé Grall, Research Project - Certified Programming in Coq, 90h (1/3 supervised), M1 and M2, IMT-Atlantique, Nantes, France

Master : Nicolas Tabareau, Homotopy Type Theory, 24h, M2 LMFI, Université Paris Diderot, France

Master : Guilhem Jaber, Verification and Formal Proofs, 18h, M1, Université de Nantes, France

8.2.2. Supervision

PhD : Simon Boulier, Extending Type Theory with Syntactical Models, IMT Altantique, 29 Nov 2018, advisor: Nicolas Tabareau

PhD in progress : Antoine Allioux, Coherent Structures in Dependent Type Theory and Higher Category Theory, Université Paris Diderot, advisors: Yves Guiraud and Matthieu Sozeau

PhD in progress : Gaetan Gilbert, A new foundation for the Coq proof assistant based on the insight of Homotopy Type Theory, IMT Atlantique, advisors: Matthieu Sozeau and Nicolas Tabareau

PhD in progress : Ambroise Lafont,Towards an unbiased approach to specify, implement, and prove properties on programming languages, IMT Atlantique, advisors: Tom Hirschowitz and Nicolas Tabareau

PhD in progress: Xavier Montillet, Rewriting theory for effects and dependent types, Univ Nantes, advisors: Guillaume Munch-Maccagnoni and Nicolas Tabareau

PhD in progress: Théo Winterhalter, Extending the flexibility of the universe hierarchy in type theory, Univ Nantes, advisors: Matthieu Sozeau and Nicolas Tabareau

PhD in progress: Igor Zhirkov, Certified Refactoring of C in the Coq proof assistant, advisors: Rémi Douence and Julien Cohen.

PhD in progress: Joachim Hotonnier, Deep Specification for Domain-Specific Modelling, advisors: Gerson Sunye (Naomod team), Massimo Tisi (Naomod team), Hervé Grall

8.2.3. Juries

- A. Mahboubi has served as reviewer for the PhD of Andrea Gabrielli, defended October 22nd at Università di Firenze.
- A. Mahboubi has served as external member on the PhD jury of Pierre Boutry, defended November 13th at Université de Strasbourg.
- A. Mahboubi has served as external member on the PhD jury of Simon Boulier, defended November 29th at IMT Atlantique.
- A. Mahboubi has served as external member on the PhD jury of Boris Djalal, defended December 3rd at IMT Atlantique.
- J. Cohen has served as external member on the PhD jury of Thibaut Girka, defended July 3rd at Université Paris Diderot.

8.3. Popularization

8.3.1. Interventions

- A. Mahboubi is working with composer Alessandro Bossetti and students of the professional high-school Lycée Michelet, on a project “Art and Mathematics”, supported by the Athenor theater.

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 was on the program committee of CADO 2018, the special session on Compiler, Architecture, Design and Optimization of the 16th International Conference on High Performance Computing and Simulation.

Michel Mauny has been a member of the program committee of the International Symposium on Image, Video and Communications (ISIVC 2018).

François Pottier was a member of the program committee of ICFP 2018, the ACM International Conference on Functional Programming.

Didier Rémy was a member of the program committee of FLOPS 2018, the 14th International Symposium on Functional and Logic Programming.

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 September 2018, Michel Mauny has been 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

In 2018, Michel Mauny was chairman of the Scientific Committee of the Caml Consortium. He organized its annual meeting in December 2018.

Since May 2018, Michel Mauny has been Chief Executive Officer of the Inria Foundation.

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*.

Didier Rémy is Inria's delegate in the pedagogical board of the *Master Parisien de Recherche en Informatique* (MPRI).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Master (M2): “Proofs of Programs”, Jean-Marie Madiot, 18 HETD, Université Paris Diderot, France.

Master (M2): “Semantics, languages and algorithms for multi-core programming”, Luc Maranget, 18 HETD, Université Paris Diderot, France.

Master (M2): “Functional programming and type systems”, François Pottier, 18 HETD, Université Paris Diderot, France.

Master (M2): “Functional programming and type systems”, Didier Rémy, 18 HETD, Université Paris Diderot, France.

Licence (L3): Jean-Marie Madiot, “Les principes des langages de programmation”, 40 HETD, École Polytechnique, France.

Master (M1): Michel Mauny, “Principles of Programming Languages”, 32 HETD, ENSTA-ParisTech, France.

Open lectures: Xavier Leroy, *Programmer = démontrer? La correspondance de Curry-Howard aujourd’hui*, 16 HETD, Collège de France, France.

10.2.2. Supervision

PhD: Vitaly Aksenov, “Synchronization Costs in Parallel Programs and Concurrent Data Structures”, ITMO University of Saint Petersburg (Russia) and Université Paris Diderot, September 26, 2018, advised by Petr Kuznetsov and Anatoly Shalyto [11].

PhD: Pierrick Couderc, “Vérification des résultats de l’inférence du compilateur OCaml”, Université Paris-Saclay, October 23, 2018, advised by Michel Mauny et Fabrice Le Fessant [34].

PhD in progress: Albin Coquereau, “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, advised 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, advised by Arthur Charguéraud and François Pottier.

PhD in progress: Glen Mével, “Towards a system for proving the correctness of concurrent Multicore OCaml programs”, Université Paris Diderot, since November 2018, advised by Jacques-Henri Jourdan and François Pottier.

PhD in progress: Naomi Testard, “Reasoning about Effect Handlers and Cooperative Concurrency”, Université Paris Diderot, since January 2017, advised by François Pottier.

PhD in progress: Thomas Williams, “Putting Ornaments into practice”, Université Paris Diderot, since September 2014, advised by Didier Rémy.

10.2.3. Juries

Xavier Leroy was a member of the jury for the Habilitation defense of Julien Signoles (Université Paris Sud, July 2018).

Xavier Leroy chaired the jury for the Ph.D. defense of Mario Pereira (Université Paris Sud, December 2018).

François Pottier was a reviewer for Steven Keuchel’s PhD thesis (Ghent University), defended on June 5, 2018.

François Pottier was a reviewer for Martin Clochard’s PhD thesis (Université Paris-Saclay), defended on March 30, 2018.

10.3. Popularization

10.3.1. Articles and contents

- For online publications (Interstices*, Images des Maths, Binaire, Wikipedia), and more widely blog articles

  Xavier Leroy wrote a short introduction to software sciences in general and to his lectures at Collège de France. This text was published by the “Binaire” blog of *Le Monde* [30].

10.3.2. Interventions

Gergö Barany gave a talk titled “Finding Missed Optimizations in LLVM (and other compilers)” at the 2018 European LLVM Developers Meeting, explaining his research on testing the quality of compiler optimizations to practitioners in compiler development.

MARELLE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Yves Bertot is member of steering committee for the conferences ITP, CPP and UITP.

Yves Bertot organized the Coq Implementor's Workshop in May in Nice, France, where Cyril Cohen, Maxime Dénès, and Enrico Tassi also brought support to newcomers.

Laurence Rideau Organized a meeting of the ANR FastRelax project in June in Sophia Antipolis. There were presentations by Sophie Bernard, Yves Bertot, Cyril Cohen, Damien Rouhling, Laurent Théry during this meeting.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Benjamin Grégoire was a Program Committee member for CSF 2018 and JFLA 2019. Enrico Tassi was a Program Committee member for CPP 2019, ITP 2018, UITP 2018, F-IDE 2018. Laurent Théry was a Program Committee member for AISC, CPP 2019, ITP 2018, and UITP 2018. Yves Bertot was a Program Committee member for AISC, CICM, FMM, and UITP.

9.1.3. Journal

9.1.3.1. Reviewer - Reviewing Activities

Laurent Théry was a reviewer for *Annals of Mathematics and Artificial Intelligence*, *Journal of Applied Logic*, and *Science of Computer Programming*. Cyril Cohen was a reviewer for *Journal of Automated Reasoning* and *Mathematical Structures in Computer Science*. Enrico Tassi was a reviewer for *ACM Transactions on Computational Logic* and *Journal of Automated Reasoning*. Yves Bertot was a reviewer for *Journal of Automated Reasoning*.

9.1.4. Invited Talks

Cyril Cohen gave an invited talk on formalizing robotics in January in Nijmegen, the Netherlands.

Cyril Cohen gave an invited talk on asymptotic reasoning in June in Pittsburgh, USA.

Cyril Cohen gave an invited talk at the workshop *Lean User Group* in November in Freiburg, Germany.

Benjamin Grégoire gave an invited talk at the "journées nationales du GDR sécurité" (national days of the CNRS research group on security) in May in Paris, France.

Benjamin Grégoire gave an invited tutorial at the CHES conference (Cryptographic Hardware and Embedded Systems) in September in Amsterdam, the Netherlands.

Enrico Tassi gave a four-hour tutorial at the EUTypes Summer School in August in Ohrid, Macedonia (https://sites.google.com/view/2018eutypesschool/home)

Enrico Tassi gave an invited talk at the ML workshop in September in Saint Louis, Missouri, USA on "ELPI: an extension language with binders and unification variables".

Yves Bertot gave an invited talk at the ICTAC conference in October in Stellenbosch, South Africa on "Formal Verification of a Geometry Algorithm: A Quest for Abstract Views and Symmetry in Coq Proofs". He also gave a half-day tutorial on Coq.

9.1.5. Leadership within the Scientific Community

We organized two one-week courses on the Coq system, both tagged as entry-level, on Coq and Coq and the Mathematical Components library.

9.1.6. Scientific Expertise

Yves Bertot was part of the review committee for the French *Haut Commissariat pour l'Évaluation de la Recherche et de l'Enseignement Supérieur* for the CNRS laboratory SAMOVAR in Evry, France.

9.1.7. Research Administration

- José Grimm is a member of the local committee for hygiene and work safety.
- Yves Bertot was a member of the "Bureau du comité des projets" until June.
- Benjamin Grégoire is a member of the committee on computer tool usage (CUMI) for the Sophia-Antipolis Méditerranée Inria center.
- Laurence Rideau was a member of the hiring committee for researchers in Sophia Antipolis.

9.2. Teaching - Supervision - Juries

9.2.1. 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 about 20 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).

Master: Yves Bertot organized a school on Coq in January, Boris Djalal and Damien Rouhling supervised the lab sessions.

Master: Laurent Théry taught 3 hours on "introduction to computer verified proof" at Ecole des Mines de Paris,

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 some lectures on computer science history.

Licence: Cyril Cohen prepares students for oral examination in a "classe préparatoire aux grandes écoles".

9.2.2. Supervision

- Yves Bertot and Cyril Cohen supervised Boris Djalal, whose doctoral thesis was defended on December 3rd.
- Yves Bertot and Cyril Cohen supervise the doctoral thesis of Damien rouhling.
- Yves Bertot and Laurence Rideau supervise the doctoral thesis of Sophie Bernard.
- Yves Bertot and Benjamin Grégoire supervise the doctoral thesis of Cécile Baritel-Ruet.

9.2.3. Juries

Enrico Tassi was a member of the Thesis jury for Andrea Gabrielli, in October at the University of Florence, Italy.

Yves Bertot was a member of the Thesis jury for Guillaume Davy, in December at the University of Toulouse and the Institut Supérieur d'Aéronautique et de l'Espace, France.

9.3. Popularization

9.3.1. Interventions

Cyril Cohen presented the work of the Marelle team at a presentation for students coming from Mediterranean regions: Meddays.

MEXICO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Matthias Függer was

- general co-chair of the IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC) 2018 (www.async2018.wien)
- general co-chair of the Workshop of Emergent Algorithms and Network Dynamics (WENDY) 2018 (wendy.paris)

Serge Haddad is a member of the steering commitee of the Petri Nets conference.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Thomas Chatain was co-chair of the program committe of ACSD 2018 interes.institute/acsd2018/.

10.1.2.2. Member of the Conference Program Committees

- Matthias Függer was a PC member of
  - the *21st IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems(DDECS 2018)*,
- Stefan Haar was a PC member of
  - the *18th International Conference on Applications of Concurrency to Systems Design(ACSD 2018)*,
  - the workshop *Algorithms and Theories for the Analysis of Event Data 2018(ATAED 2018)*, and
  - the *International Workshop on Petri Nets and Modeling(PeMod '18)*.
- Laurent Fribourg was a PC member of
  - *Model-Based Design of Cyber Physical Systems* (CyPhy'18), October 4-5, 2018, Torino, Italy,
  - *12th International Conference on Reachability Problems* (RP'18), September 24-26 2018, Marseille, France,
  - *8th International Conference on New Computational Methods for Inverse Problems* (NCMIP'18), Ecole normale supérieure Paris-Saclay, France.
- Serge Haddad was a PC member of
  - *12th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2018)*, Grenoble, France, September 2018
  - *5th International Symposium on Formal Approaches to Parallel and Distributed Systems (4PAD 2018)*, Orléans, France, July 2018

10.1.2.3. Reviewer

- Matthias Függer reviewed for Automatica, ASYNC'18, DDECS'18, Philisophical Transactions, DISC'18, PODC'18, SIROCCO'18, STACS'18.
- Stefan Schwoon reviewed for MFCS and FSTTCS.

- Stefan Haar reviewed for FOSSACS 2019.

10.1.3. Journals

10.1.3.1. Member of the Editorial Boards

- Matthias Függer is guest editor for the special issue *Selected Papers from the 24th IEEE International Symposium on Asynchronous Circuits and Systems - ASYNC 2018*
- Stefan Haar is an associate editor for *Journal of Discrete Event Dynamic Systems*

10.1.3.2. Reviewer - Reviewing Activities

- Thomas Chatain reviewed for *Journal of Discrete Event Dynamic Systems*, *Transactions of the Society for Modeling and Simulation International*.
- Stefan Schwoon reviewed for *Journal of Discrete Event Dynamic Systems*, *Acta Informatica*, *ACM Transactions on Programming Languages and Systems*.
- Stefan Haar reviewed for *Scientific Annals of Computer Science* and *IEEE Transactions on Automatic Control*.

10.1.4. Invited Talks

- Serge Haddad gave an invited talk on “Time and Stochastic Petri Nets” at the tutorials of Petri Nets 2018, the 25th June 2018, Bratislava, Slovakia
- Matthias Függer gave an invited talk at ACSD’18 on "Challenges of circuit design: Circuits as robust distributed algorithms"

10.1.5. Scientific Expertise

- Stefan Schwoon acted as reviewer for the ERC 2018 Starting Grant call.
- Serge Haddad was expert for the allocation of the grants ”Prime d’Investissement Recherche de l’Université” of Sorbonne Université

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Note: we only list the teaching activities of researchers here, not those of our assistant and full professors.

Licence: Stefan Haar taught one half of the L3 course on formal languages (18 h EQ TD) at ENS Paris-Saclay.

Master: Matthias Függer and Stefan Haar each taught a module of 10 h EQTD in the *Jaques Herbrand* master MI course *Introduction à la recherche*.

Laurent Fribourg taught one half of M2 course on “Hybrid Automata” at MPRI (Master Parisien de Recherche en Informatique).

10.2.2. Supervision

PhD:

- Thomas Chatain is the supervisor of the PhD thesis of Mathilde Boltenhagen.
- Stefan Haar is the supervisor of the PhD theses of
  - **Juraj Kolcˇák** Unfoldings and Abstract Interpretation for Parametric Biological Regulatory Networks, started in March 2017, and of
  - **Hugues Mandon** on *Computational models and algorithms for the prediction of cell reprogramming strategies*, started on Oct. 1st,

  both at ENS Paris-Saclay.
- Laurent Fribourg is the supervisor of the PhD theses of

  - **Adnane Saoud***Compositional controller synthesis for cyber-physical systems*, started in October 2016, co-supervised by Antoine Girard (CentraleSupelec), funded by Digicosme projet Emergence Codecsys
  - **Jawher Jerray***Formal analysis of real-time systems*, started in October 2018, co-supervised by Etienne André (Paris 13), funded by University Paris 13, ED Galilée.
- Serge Haddad is the supervisor of the PhD thesis of Igor Khmelnitsky on Machine Learning and Verification of Infinite-state Systems co-supervised with Alain Finkel.

10.2.3. Juries

- Thomas Chatain reviewed the PhD thesis of Thi Thanh Huyen Nguyen, directed by Laure Petrucci and defended at Université Paris 13 in December 2018.
- Stefan Schwoon reviewed the PhD thesis of Adrien Pommellet, directed by Tayssir Touili and defended at Université Paris 13 in July 2018. He also acted as examinator for the PhD thesis of Huu Vu Nguyen.

10.3. Popularization

Laurent Fribourg was interviewed by *L'Édition de l' Université Paris-Saclay* in: "La cyberphysique prépare l'usine de demain", May 2018.

10.3.1. Internal or external Inria responsibilities

- Laurent Fribourg is Head of Institut Farman (FR 3311 CNRS & ENS Paris-Saclay).
- Serge Haddad is Head of the Computer Science Department of ENS Paris-Saclay.
- Stefan Haar is the president of Inria's COST-GTRI.

MOCQUA Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Emmanuel Jeandel organized with three other colleagues the “Jeunes-Chercheurs” school of GDR IM.
- Frédéric Dupuis and Simon Perdrix organized the “Journées informatique quantique” in Nancy, Novembre 2018.
- Nazim Fatès and Irène Marcovici organised a “Journée Charles Hermite” on the theme "Cellular automata and dynamics on networks" (Nancy, Decembre 2018).

9.1.1.2. Member of the Organizing Committees

- Mathieu Hoyrup is member of the Steering Committee of the Conference Series *Computability in Europe* (CiE) for the period 2017-2021.
- Simon Perdrix is in the Scientific Board of the Colloquium IQFA (Montpellier, Novembre 2018).
- Nazim Fatès is a member of the steering committee of the Summer Solstice Conference on Discrete Models of Complex Systems.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Mathieu Hoyrup was PC member of the workshop Continuity, Computability, Constructivity - From Logic to Algorithms (CCC) 2018, Faro, September 2018.
- Emmanuel Jeandel and Simon Perdrix were PC members of MCU 2018 (https://mcu2018.lacl.fr/).
- Romain Péchoux was PC member of the workshop DICE 2018 (http://cl-informatik.uibk.ac.at/users/zini/events/dice18/).
- Frédéric Dupuis was PC member of QCrypt 2018 (http://2018.qcrypt.net/) and QIP 2019 (http://jila.colorado.edu/qip2019/).
- Nazim Fatès was a PC member of Automata 2018 and ACRI 2018.

9.1.2.2. Reviewer

- Mathieu Hoyrup reviewed articles for LICS, CiE and ICALP.
- Romain Péchoux reviewed articles for DICE, ISMVL and CSL.
- Frédéric Dupuis reviewed articles for QCrypt 2018, QIP 2019, CRYPTO 2018, and AQIS 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Emmanuel Jeandel is member of the editorial board of RAIRO-ITA (Revue d’Automatique, d’Informatique et de Recherche Opérationnelle: Informatique théorique et applications).
- Romain Péchoux is guest editor for a Theoretical Computer Science special issue on Implicit Computational Complexity (https://www.journals.elsevier.com/theoretical-computer-science/call-for-papers/mplicit-computational-complexity).
- Nazim Fatès is a member of the editorial board of the *Journal of cellular automata*.

9.1.3.2. Reviewer - Reviewing Activities

- Mathieu Hoyrup reviewed articles for Discrete and Continuous Dynamical Systems, Information and Computation, and Theoretical Computer Science.
- Romain Péchoux reviewed articles for Information Processing Letters, Journal of Automated Reasoning and Theoretical Computer Science.
- Frédéric Dupuis reviewed articles for Nature Communications, Quantum, IEEE Transactions on Information Theory, Physical Review A, Journal of Physics A, and the Journal of Mathematical Physics.
- Nazim Fatès reviewed articles on cellular automata for the *Journal of cellular automata*, *Physical Review A*, *Chaos, Solitons & Fractals* and *Informatica*.

9.1.4. Invited Talks

- Mathieu Hoyrup was invited to give a talk at the special session Continuous Computation at CiE 2018.
- Nazim Fatès was invited to give a talk on artificial intelligence in the "Colloque Cathy Dufour 2018" held in Nancy in November 2018.

9.1.5. Scientific Expertise

- Romain Péchoux was expert for the European Commission H2020 Marie Skłodowska-Curie Individual Fellowships.
- Nazim Fatès served as an expert for the Chilean national institute of research CONICYT.

9.1.6. Research Administration

- Simon Perdrix is the Scientific Secretary of the CoNRS Section 6. He was in the panel of the CR and DR recruitments at CNRS section 6.
- Frédéric Dupuis is on the board of the Fédération Charles-Hermite (Université de Lorraine).
- Emmanuel Hainry is a member of the CNU Section 27.
- Nazim Fatès is the vice-chair of the IFIP Working group 1.5 on cellular automata and discrete complex systems.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence
  - Isabelle Gnaedig:
    - To the limits of the computable, 6 hours, Opening course-conference of the collegium "Lorraine INP", Nancy, France
  - Emmanuel Hainry:
    - Operating Systems, 30h, L1, IUT Nancy Brabois
    - Algorithmics, 40h, L1, IUT Nancy Brabois
    - Dynamic Web, 60h, L1, IUT Nancy Brabois
    - Databases, 30h, L1, IUT Nancy Brabois
    - Object Oriented Languages, 16h, L2, IUT Nancy Brabois
    - Complexity, 30h, L2, IUT Nancy Brabois
  - 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
    - Data Compression, 30h, L2 Informatique
    - Algorithmics and Programming 4, 30h, L3 Informatique
    - Modeling Using Graph Theory, 30h, L3 Informatique
    - Networking, 15h, L3 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
    - Algorithmic complexity, 30h, L3 MIAGE, IGA Rabat, Morocco.
- 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
  - Nazim Fatès:
    - Systèmes distribués adaptatifs, 10h, Master 2, informatique.
    - Agents intelligents et collectifs, 15h, Master 1, sciences cognitives.

9.2.2. Supervision

- PhD in progress: Renaud Vilmart, "Langages graphiques pour calculer et raisonner en quantique", Start: October 2016, Advisors: Emmanuel Jeandel and Simon Perdrix.
- PhD in progress: Titouan Carette, "Langage diagrammatique pour l'ordinateur quantique", Start: October 2018, Advisors: Emmanuel Jeandel and Simon Perdrix.
- PhD in progress: Pierre Mercuriali, "Calcul à base de médiane et structures médianes pour la classification", Start: October 2016, Advisors: Miguel Couceiro and Romain Péchoux.
- PhD in progress: Robert Booth, "Formalismes pour la vérification de technologies quantiques", Start: November 2018, Advisors: Damian Markham and Simon Perdrix.

9.2.3. Juries

- Emmanuel Jeandel reviewed the PhD thesis of Silvère Gangloff (Aix-Marseille Université - Université Toulouse III).
- Simon Perdrix was examiner for the PhD thesis of Alex Bredariol Grilo (IRIF, Université Paris Diderot), April 27 2018.
- Frédéric Dupuis was examiner for the PhD thesis of Christoph Hirche (Universitat Autònoma de Barcelona), May 9, 2018.

9.3. Popularization

9.3.1. Articles and contents

Nazim Fatès and Irène Marcovici presented an article on cellular automata in the wide audience scientific magazine *La recherche* [23]. This article appeared in an issue dedicated to "chaos and complexity" (July-August 2018).

Simon Perdrix has been one of the editors of the ERCIM news special issue on Quantum Computing.

9.3.2. Education

Nazim Fatès participated in a day of training destined to high school teachers of the “Académie de Poitiers” with a conference and discussions with the participants. The meeting was held on April 25, 2018, in the Lycée Victor Hugo of Poitiers and was also followed on the internet by teachers located abroad (DOM-TOM).

9.3.3. Interventions

Nazim Fatès participated to a debate for a large public on the theme "Space and artificial intelligence" in the Cité des sciences et de l’industrie in Paris. This debate was part of a series of events dedicated to celebrations of the fiftieth year of the film *2001, A space Odyssey*.

Nazim Fatès joined the Pariscience Festival for animating a debate on artificial intelligence with high-school students of the region of Paris. The discussion, held together with a researcher from the INSERM institute, followed the projection of the film *IA : votre nouveau cerveau* and a collective game to debate on the question of artificial intelligence.

Nazim Fatès participated in an open debate on the theme: “L’intelligence artificielle, quel avenir pour les artistes et créateurs d’aujourd’hui ?”. This debate was held in conjunction with the RING Theater Festival in Nancy (Rencontres Internationales des Nouvelles Générations) in April 2018.

Nazim Fatès participated in an open debate on the general theme of joining science and art in conjunction with the exposition “Retina Pictonique” which was held in July 2018 in Toulouse in the CEMES Laboratory.

Nazim Fatès participated in an open debate on the theme “L’intelligence artificielle est-elle vraiment maligne ?” in the Shadok fab-lab of Strasbourg. The debate gathered more than a hundred persons and was preceded by an interview in the magazine *Rue 89 Strasbourg*.

9.3.4. Internal action

Nazim Fatès gave a talk on artificial intelligence in the *Café-In* meeting, one of the Inria Nancy Grand-Est series of talks destined to all the employees of the laboratory (March 13, 2018).

Frédéric Dupuis also gave a *Café’In* talk on quantum computing (February 13, 2018).

PARSIFAL Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

D. Miller is the General Chair of LICS (Logic In Computer Science), starting July 2018.

9.1.1.2. Member of the Organizing Committees

D. Miller is on the Steering Committee for the FSCD conference series and the CPP conference series.

D. Miller is a member of the SIGLOG advisory board, starting November 2015.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

B. Accattoli co-chaired LSFA 2018: 13th Workshop on Logical and Semantic Frameworks with Applications, Fortaleza, Brazil, September 26-28, 2018.

G. Scherer chaired ML2018: the ML Family Workshop 2018 in Saint Louis, US, on Friday September 28th 2018.

L. Straßburger chaired TYDI 2018: Workshop on “Twenty Years of Deep Inference” in Oxford July 7, 2018.

9.1.2.2. Member of the Conference Program Committees

B. Accattoli was on the PPDP 2018 Program Committe: 20th International Symposium on Principles and Practice of Declarative Programming, Frankfurt, Germany, 3–5 September 2018.

S. Graham-Lengrand was on the LFMTP 2018 Program Comittee: Workshop on Logical Frameworks and Meta-Languages: Theory and Practice, Oxford, UK, 7 July 2018.

L. Straßburger was on the PC for LACompLing 2018: Symposium on Logic and Algorithms in Computational Linguistics, Stockholm, 28–31 August 2018

D. Miller was on the program committee for IJCAR-2018: 9th International Joint Conference on Automated Reasoning, Oxford, 14-17 July 2018.

D. Miller was a member of the jury for selecting the 2018 Ackermann Award (the EACSL award for outstanding doctoral dissertation in the field of Logic in Computer Science).

Member of the EATCS Distinguished Dissertation Award Committee since March 2013.

G. Scherer was on the POPL 2019 Program Committee: Principles Of Programming Languages, 13-19 January 2019 Cascais/Lisbon, Portugal

9.1.2.3. Reviewer

G. Scherer reviewed for Computer Science Logic (CSL).

L. Straßburger was reviewer for the following conferences:

- LICS 2018
- IJCAR 2018
- FSCD 2018
- AiML 2018
- ARQNL 2018

B. Accattoli reviewed for LICS 2018, FSCD 2018, PPDP 2018, LSFA 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

D. Miller is on the editorial board of the following journals:

- Journal of Automated Reasoning
- Journal of Applied Logics

9.1.3.2. Reviewer - Reviewing Activities

G. Scherer reviewed for Mathematical Structures in Computer Science (MSCS).

L. Straßburger was reviewer for the following journals:

- Transactions on Computational Logic, ToCL (2x)
- Logical Methods in Computer Science, LMCS
- Mathematical Structures in Computer Science, MSCS
- Journal of Logic, Language and Information, JLLI
- Journal of Automated Reasoning, JAR
- Notre Dame Journal of Formal Logic, NDJFL

B. Accattoli reviewed for Logical Methods in Computer Science (LMCS) and Theoretical Computer Science (TCS).

9.1.4. Invited Talks

S. Graham-Lengrand gave an invited talk at the JFLA 2018 (January), and an invited lecture series at the 8th Summer School on Formal Techniques (May).

B. Accattoli gave an invited talk at the *IFIP Working Group 1.6: Rewriting* on July 8 2018 in Oxford, Uk.

D. Miller was an invited speaker and panelist at the Workshop on Proof Theory and its Applications, 6–7 September 2018 in Ghent, Beligum.

D. Miller gave a colloquim talk at the Technical University of Vienna on 31 October 2018 and at the Cyber Security Lab, NTU, Singapore, 21 March 2018.

9.1.5. Scientific Expertise

G. Scherer participated to a scientific expertise of the implementation of the Tezos blockchain – implemented in OCaml.

9.1.6. Research Administration

L. Straßburger was reviewer for the NWO (Netherlands Organisation for Scientific Research).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : G. Scherer, Programmation Fonctionnelle, 50, L1, Paris 8 (Vincennes / Saint Denis), France

Licence : K. Chaudhuri, Programmation avancée en OCaml, 40 hours eq TD, L3, École polytechnique, France

Bachelor : K. Chaudhuri, Computer programming, principal instructor, École polytechnique, France (This program has no direct equivalent in the traditional French university system; the closest would be L1.)

Licence: S. Graham-Lengrand, “*INF412: Fondements de l’Informatique: Logique, Modèles, Calcul*”, 32 hours eq. TD, L3, École Polytechnique, France.

Master: S. Graham-Lengrand, “*INF551: Computational Logic*”, 45 hours eq. TD, M1, École Polytechnique, France.

Master: B. Accattoli, “*Logique linéaire et paradigmes logiques du calcul*”, 18 hours eq. TD, M2, Master Parisien de Recherche en Informatique (MPRI), France.

Master: D. Miller, “*Logique linéaire et paradigmes logiques du calcul*”, 18 hours eq. TD, M2, Master Parisien de Recherche en Informatique (MPRI), France.

Summer School: B. Accattoli, “The Complexity of Beta-reduction”, 4.5h, International School on Rewriting (ISR) 2018, Cali, Colombia.

9.2.2. Supervision

PhD : Sonia Marin, Modal Proof Theory through a Focused Telescope, Université Paris-Saclay, 30 January 2018, encadrant(s): Lutz Straßburger, Dale Miller.

PhD in progress: Ulysse Gérard and Matteo Manighetti supervised by Dale Miller.

PhD in progress: François Thiré (since 1st October 2016), supervised by S. Graham-Lengrand (joint with G. Dowek).

PhD in progress: Maico Leberle supervised by Dale Miller and Beniamino Accattoli.

9.2.3. Juries

D. Miller was the a reporter for the PhD juries of Michael Lettmann (TU Vienna, 30 October 2018)

9.3. Popularization

L. Straßburger serves as member of the “commission développement technologique (CDT)” for Inria Saclay–Île-de-France (since June 2012).

F. Lamarche was site co-ordinator for the Activity Report for Inria Saclay–Ile-de-France.

9.3.1. Interventions

G. Scherer and M. Manighetti participated the “Fête de la Science” exhibit at Inria Saclay on the whole day of October 11th, 2018. They manned an activity on sorting algorithms for colored plastic pieces.

9.3.2. Internal action

G. Scherer spoke at the “Unithé ou café” meeting, a Saclay-internal popularization meeting, on February 1st, 2018.

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 organised a Day of Hommage to the memory of Maurice Nivat on February 6, 2018, at University Paris 7.

Alexis Saurin organised and co-chaired with David Baelde the Paris workshop in Oxford, UK, July 7-8th 2018, collocated with FLoC 2018.

Matthieu Sozeau co-organised and co-chaired with Nicolas Tabareau the Coq Workshop 2018 in Oxford, UK, July 8th 2018, collocated with FLoC 2018.

8.1.1.2. Member of the Organising Committees

Yves Guiraud organised with Philippe Malbos (Univ. Lyon 1) and Samuel Mimram (École Polytechnique) the fourth edition of the workshop HDRA (Higher-Dimensional Rewriting and Algebra) in July 2018 in Oxford.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

Hugo Herbelin was a member of the program committee of the conference POPL 2019.

Yann Régis-Gianas was a member of the program committee of the conference PPDP 2018.

Yann Régis-Gianas was a member of the program committee of the conference JFLA 2019.

Matthieu Sozeau was member of the program committee of the conference Interactive Theorem Proving 2018 which took place in Oxford during FLoC 2018 and the 13th Workshop on Logical and Semantic Frameworks with Applications, which took place in Fortaleza, Brazil, September 26-28, 2018.

8.1.2.2. Member of the Conference Steering Committees

Pierre-Louis Curien is member of the steering committee of the international workshop Games for Logic and Programming Languages (GaLop).

Hugo Herbelin is a member of the steering committee of the conference TYPES.

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 talks on the legacy of Maurice Nivat at two special events organised to honour his memory: special sessions in the Journées du GDR IM (Ecole Polytechnique, May 2018), and at ICALP 2018 (Prague, July 2018).

Eric Finster gave an invited talk at the annual meeting of the GDR Topologie in Montpellier in October entitled "The Cotopological Tower".

Hugo Herbelin gave an invited talk on computing with Gôdel's completeness theorem using side effects at the workshop Proof, Computation and Complexity in Bonn, July 2018.

Yann Régis-Gianas gave an invited talk about copatterns in OCaml at the "Logique, Types et Preuves" workshop of the GDR GPL.

Matthieu Sozeau gave an invited talk on "The Predicative, Polymorphic, Cumulative Calculus of Inductive Constructions" at the TYPES 2018 International Conference on Types for Proofs and Programs in Braga, Portugal, 18-21 June 2018.

Matthieu Sozeau gave an invited seminar entitled "Programmer en Coq" at the Collège de France, on December 12th 2018, part of Xavier Leroy's lectures on the Curry-Howard Isomorphism.

Théo Zimmermann was invited to give a talk in the First international workshop on Empirical Answers to Questions of Software Engineering to present his work on the impact of switching bug trackers [60].

8.1.5. Scientific Expertise

Pierre-Louis Curien has been an expert for a hiring committee for an assistant professor position in Logic, Computation and Programming at Stockholm University (June 2018).

Hugo Herbelin has been a reviewer for FWF (Austrian research funding agency) and NKFI (Hungarian research funding agency).

8.1.6. Research Administration

Pierre-Louis Curien is a member of the Scientific Council of the CIRM (Centre International de Rencontres Mathématiques).

Pierre-Louis Curien and Yves Guiraud are members of the scientific council of the Computer Science department of University Paris 7.

Yves Guiraud is the head of the "Preuves, Programmes et Systèmes" (PPS) pole of the IRIF laboratory (since April 2016), and a member of the IRIF direction council (since September 2017).

Yann Régis-Gianas is a member of the Executive Comitee of the OCaml Foundation, acting as a representative of the teaching community.

In collaboration with Emmanuel Chailloux (UPMC), Yann Régis-Gianas is organising the next four years of IRILL, an initiative about innovation in free software.

8.1.7. Presentation of papers

Pierre-Louis Curien gave a talk at the Conference "Topology in Australia and South Korea 2018", Pohang (https://cgp.ibs.re.kr/conferences/Topology_in_Australia_and_South_Korea) in April 2018 ('A syntactic approach to opetopes').

Yann Régis-Gianas gave talks to present "Morbig", a static parser for POSIX Shellat at FOSDEM 2018 in Brussels, at MiniDebConf 2018 and at SLE 2018 in Boston.

Yann Régis-Gianas gave a talk at OCaml 2018 in St Louis to present Learn-OCaml, a project to support the teaching of OCaml worldwide.

Yann Régis-Gianas gave a talk at JFLA 2018 to present his work about extending OCaml with Copatterns.

Exequiel Rivas gave a talk on relating interfaces for computational effects at the Seventh Workshop on Mathematically Structured Functional Programming (MSFP 2018) in July 2018.

Exequiel Rivas gave a talk on relating interfaces for computational effects at the First Symposium on Compositional Structures (SYCO I) in September 2018.

Matthieu Sozeau gave a talk and presented a poster at PEPM 2018 on Equations, gave a talk on Typed Template Coq at CoqPL 2018, along with the traditional Coq developer session. These events were co-located with POPL 2018 in Los Angeles, CA in January 2018.

8.1.8. Talks in seminars

Eric Finster gave a talk about the implementation of Catt, a proof assistant for Maltsinotis-style higher categories at the Journées pi.r2 (Fontainebleau, june 2018).

Eric Finster gave a talk on “Towards Higher Universal Algebra in Dependent Type Theory” in the working group on Higher Categories, Polygraphs and Homotopy, during the Journées PPS (November 2018).

Eric Finster gave a talk during the HoTTest Electronic Seminar on "Towards Higher Universal Algebra in Type Theory".

Eric Finster gave a talk entitled "Left Exact Modalities in Type Theory" at the Cambridge Logic and Semantics Seminar (March 2018).

Hugo Herbelin gave a talk on computing with Gödel’s completeness theorem at the seminar of the Logic team of the IMJ-PRG Paris 6 - Paris 7 lab.

Pierre Letouzey gave two talks on “Un problème d’Hofstadter pour ses lecteurs curieux” during the Journées pi.r2 (Fontainebleau, june 2018) and the Journées PPS (November 2018).

Jean-Jacques Lévy gave a talk at the IRIF Verification seminar (January 8) entitled "Proofs of graph algorithms with automation and their readability".

Jean-Jacques Lévy gave a talk at the VIP ISCAS-Inria workshop (Irif, November 19-22) entitled "Comparing a Formal Proof in Why3, Coq and Isabelle".

Yann Régis-Gianas gave a talk at Gallium seminar to present "Morbig", a static parser for POSIX Shell.

Exequiel Rivas gave a talk on “Arrows: from programming to semantics” at the Laboratoire d’Informatique de Paris Nord (LIPN), September 2018.

Exequiel Rivas gave a talk on “Interaction from monadic interfaces” during the Journées PPS, November 2018.

Exequiel Rivas gave a talk on “Interaction from monadic interfaces” at the Prosecco seminar, December 2018.

Alexis Saurin gave a talk at I2M seminar in the "logique de la programmation" group entitled "logical-by-need".

Alexis Saurin gave a talk at the VIP ISCAS-Inria workshop (Irif, November 19-22) entitled "On non-wellfounded proofs and cuts in linear logic with fixed points."

Matthieu Sozeau gave a talk on the MetaCoq Project at the VALS seminar, LRI, October 2018.

Matthieu Sozeau gave a talk on “A universe of strict propositions“ during the Journées PPS, November 2018.

8.1.9. Attendance to conferences, workshops, schools,...

Hugo Herbelin attended TYPES 2018 in Porto (June), the Coq Implementors Workskop in Nice (May 2018), FLoC in Oxford (July 2018), the GPL working group in Marseille (October 2018), the Scalp working group in Saclay (November 2018).

Hugo Herbelin gave a talk on cubical type theory at the workshop Types, Homotopy Type theory and Verification (June 2018), on computing with Markov's principle at the workshop Proof and Computation (July 2018), on a constructive proof of the axiom of dependent choice compatible with classical logic at the workshop Constructive Mathematics (August 2018), all workshops of the special trimester on types, sets and constructions in Bonn. He gave a talk on the reverse mathematics of Gödel's completeness theorem and on the computational contents of Henkin's proof at the seminar of the trimester.

Hugo Herbelin gave a talk on cubical type theory at the TYPES conference (June 2018).

Hugo Herbelin gave a talk on the cubical type structure of cubical type theory at the HoTT-UF workshop in Oxford, July 2018.

Jean-Jacques Lévy attended the Coq Winter School 2018-2019 (SSReflect & MathComp) at Inria Sophia-Antipolis (November 2018).

Yann Régis-Gianas attended JFLA 2018, OCaml 2018, SPLASH 2018, FOSDEM 2018 and MiniDebConf 2018.

Exequiel Rivas attended to MSFP 2018 and SYCO I.

Alexis Saurin attended FLoC 2018 in Oxford.

Matthieu Sozeau attended POPL in Los Angeles, CA (January 2018), the Coq Implementors Workshop in Nice (May 2018), the TYPES Conference in Braga, Portugal (June 2018), FLoC in Oxford (July 2018) and ICFP in St Louis, MI (September 2018).

Théo Zimmermann attented FOSDEM in Brussels (February 2018), the Coq Implementors Workskop in Nice (May 2018), FLoC in Oxford (July 2018), OpenSym in Paris (August 2018) and the EAQSE workshop in Villebrumier (November 2018).

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 2018 were Rodolphe Lepigre (Practical Curry-Style using Choice Operators, Local Subtyping and Circular proofs), Armaël Guéneau (A Fistful of Dollars: Formalising Asymptotic Complexity Claims via Deductive Program Verification), Jérôme Siméon (Specifying and compiling domain specific languages using Coq: Three case studies), Laura Fontanella 'Axiom of choice in classical realisabiity), Adrien Guatto (A Generalised Modality for Recursion), Hadrien Batmalle (Preservation of properties of the original model in classical realisability), Raphaël Cauderlier (Tactics and certificates in Meta Dedukti).

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 (Univ. Nanterre) 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). Pierre-Louis Curien taught a course on the Foundations of Programming Languages at East China Normal University (12 hours, November 2018).

Master: Hugo Herbelin teaches with Nicolas Tabareau the course on Homotopy Type Theory at the LMFI.

Master: Pierre Letouzey teaches two short courses to the LMFI Master 2 students : "Programming in Coq" 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 and a course on computed-aided formal proofs to M1 students).

Master: Yann Régis-Gianas took part in the MPRI course entitled “Type systems”: he gave a 12-hour course about generalised algebraic data types, higher-order Hoare logic and dependently typed programming.

Master: Alexis Saurin 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.

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 gave a guest lecture on dependent pattern-matching and Equations at the University of Saarland in April 2018.

Matthieu Sozeau gave an introductory lecture on Dependent Type Theory at the EUTYPES summer school in Ohrid, Macedonia, in August 2018.

8.2.2. Supervision

Guillaume Claret defended his PhD on “Programmation avec effets en Coq” on 18 September 2018 (supervised by Hugo Herbelin and Yann Régis-Gianas). Note that the dissertation was completed in 2015 but Guillaume Claret moved in the meantime to a private company and the defense has been delayed.

PhD (completed): Thibaut Girka defended his PhD on "Differential Program Semantics" on the 3rd of July 2018, supervised by Roberto Di Cosmo and Yann Régis-Gianas.

PhD (abandoned): Cyprien Mangin, Dependent Pattern-Matching, induction-induction and higher inductive types (started in September 2015), supervised by Matthieu Sozeau and Bruno Barras. Cyprien Mangin left for industry.

PhD in progress: Théo Zimmermann (started in September 2016), supervised by Hugo Herbelin.

PhD in progress: Cédric Ho Thanh (started in September 2017), on Opetopes for higher-dimensional rewriting and koszulity, supervised by Pierre-Louis Curien and Samuel Mimram.

PhD in progress: Antoine Allioux (started in February 2018), on the formalisation of algebraic structures in type theory, supervised by Yves Guiraud and Matthieu Sozeau.

PhD in progress: Abhishek De (started in october 2018), on fixed point logics, structures for infinite proofs and their finite representations, supervised by Alexis Saurin.

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 Yves Guiraud and Samuel Mimram.

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 member of the jury of the PhD thesis of Clovis Eberhard (Université Savoie Mont Blanc), defended in June 2018.

Hugo Herbelin was a member of the jury of the PhD thesis of Andrea Vezzosi (University of Göteborg, Sweden), defended in September 2018.

Hugo Herbelin was a member of the jury of the PhD thesis of Guillaume Claret (University of Paris-Diderot), defended in September 2018.

Hugo Herbelin was referee for the PhD thesis of Simon Boulier (University of Nantes), defended in November 2018.

Hugo Herbelin was president of the jury of the PhD thesis of Pierre Cagne (University of Paris Diderot), defended in December 2018.

Yann Régis-Gianas is a member of the jury of the competitive examination for the entrance to the Ecoles Normales Supérieures and the Ecole Polytechnique.

Matthieu Sozeau was member of the jury of the PhD thesis of Amin Timany (KU Leuven, Belgium), defended in April 2018.

8.3. Popularisation

Pierre-Louis Curien gave a talk in the Lycée Georges Dumézil (Vernon, Eure, May 2018) on computer bugs and their prevention, on the occasion of the 50th anniversary of this high school.

Jean-Jacques Lévy is member of the Inria-Alumni’s executive committee (4 meetings in 2018) and organised the session about the Transparency of Algorithms (November 12).

Jean-Jacques Lévy was invited by the French Academy of Sciences to participate to the 2018 Hangzhou International Human Resources Exchanges and Cooperation Conference (Hangzhou, November 9-12).

Yann Régis-Gianas co-organised the “Journée Francilienne de Programmation”, a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS).

8.3.1. Education

Yann Régis-Gianas is the project leader of the "Learn-OCaml" project whose purpose is to support teaching the OCaml programming language worldwide.

8.3.2. Internal action

- Science outreach towards services (DPEI, STIP...)

  Jean-Jacques Lévy talked about “L’informatique en 4 temps” at the Alumni-UniThé seminar at Inria Bordeaux (October 10).

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 General Chair of CARI 2018, Stellenbosch, South Africa.
- Hervé Marchand is a member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. Hervé Marchand is a member of the steering committee of MSR (modélisation de systèmes réactifs) since 2012 and became the president of this steering committee in November 2017;
- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the Summer School MOVEP (*Modélisation et Vérification des Processus Parallèles*).

10.1.1.2. Member of the Organizing Committees

Nicolas Markey coorganized the 6th Workshop SR 2018 (Oxford, 7-8 july 2018).

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Hervé Marchand served on the Program Committee of WODES 2018
- Éric Badouel was member of the program committees of VECOS 2018, ATAED 2018, CARI 2018, ICTAC 2018.s
- Loïc Hélouët was member of the program Comitee of ACSD'2018.
- Thierry Jéron served on the Program Committees of the following international conferences: SAC-SVT 2018, TAP 2018.
- Nathalie Bertrand was a member of the PC of the following international events: FoSSaCS'18, ICALP'18, Highlights'18, MoRe'18 and RP'18.
- Ocan Sankur was a member of the PC of FORMATS'18 and SYNT'18.

10.1.2.2. Reviewer

In 2018, members of SUMO reviewed submissions for following conferences: VECOS, ATAED, CARI, ICTAC, CONCUR, SOFSEM, FOCS, ATVA, VMCAI, ICALP, SAC-SVT, TAP, ACSD, MFCS, STACS, WODES, HSCC, FSTTCS, CSL, AAMAS, TACAS, FoSSaCS, LICS, PODC, MORE, RP.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Éric Badouel is co-editor-in-Chief of ARIMA Journal.

10.1.3.2. Reviewer - Reviewing Activities

In 2018, members of SUMO reviewed submissions for following journals: Automatica, Fundamenta Informaticae, Information and Computation, The Scientific Annals of Computer Science, Science of Computer Programming, ACM Transactions on Computational Logic, ACM Transactions on Embedded Computing Systems, Journal of Systems and Software, Mathematical Review (MathSciNet), Journal of Discrete Event Dynamical Systems, Formal Methods in System Design, Software Testing, Verification and Reliability, Journal of Logic and Computation, IEEE Transactions on Automatic Control, PLoS one, Performance Evaluation, Artificial Intelligence, Journal of Logic and Algebraic Methods in Programming, Logical Methods in Computer Science, ACM Transactions on Modeling and Computer Simulation, Journal of Systems and Software.

10.1.4. Invited Talks

Loïc Hélouët was invited to give a talk at IIT Delhi on hyperlogics on November 2018.

10.1.5. Leadership within the Scientific Community

Nathalie Bertrand is the co-head of the *Groupe de Travail Verif* (together with Pierre-Alain Reynier (LIS, Marseille)) which is a part of *GDR Informatique Mathématique (GDR-IM).*

10.1.6. Scientific Expertise

- Eric Badouel was member of the jury discerning the Ibni Prize.
- Thierry Jéron was a reviewer for ANR.
- Blaise Genest was a reviewer for Austrian Academy of Sciences.
- Nathalie Bertrand was a reviewer for Thelam Fundand FWO (Belgium).
- Éric Fabre was a reviewer for the Ministry of Research, in the "Credit Impot Recherche" initiative.

10.1.7. Research Administration

- 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 just started in 2017, 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 SAPIENS.
- Loïc Hélouët is a representative of researchers in the Comité de Centre of Inria Rennes. He is also part of the bureau of the Comité de Centre, leads a working group of the comité and contributes to another. In 2018, he joined the COST-GTRI, who is in charge of evaluation of international programs such as Inria associated teams. He is the principal investigator for the french side of the EQUAVE associated team. He leads the P22 projects with Alstom Transport and is responsible for Workpackage 2 of the Headwork ANR project.
- Hervé Marchand is chairman of the *Comission des utilisateurs des moyens informatiques* (CUMI) in Rennes and member of the *Action de développement technologique*(ADT) commission in Rennes.
- Thierry Jéron is a Member Committee Substitute for COST IC1402 ARVI (Runtime Verification beyond Monitoring). He is a member of the IFIP Working Group 10.2 on Embedded Systems. He is a member of the *Comité d'orientation scientifique* (COS) Prospective of Irisa Rennes and a member of the Comité de Centre of Inria Rennes. Since 2016 he is *référent chercheur* for the Inria-Rennes research center.
- Nathalie Bertrand is elected member of the Conseil National des Universités, section 27 (computer science).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Nathalie Bertrand, Advanced Algorithms (ALGO2), 20h, L3, Univ Rennes 1, France;

Licence: Nathalie Bertrand, Theory of Rational Languages (THLR), 26h, EPITA 2nd year, Rennes, France.

Licence: Loïc Hélouët, JAVA and algorithms, L2, 40h, INSA de Rennes, France.

Licence: Loïc Hélouët, Practical studies (development of a small project), 8h, INSA de Rennes, France.

Master: Loïc Hélouët, Algorithms, 2h, Agrégation, ENS Rennes, France;

Master: Nicolas Markey, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;

Master: Nicolas Markey, Algorithms, 14h, Agrégation, ENS Rennes, France;

Master : Nathalie Bertrand, Language Theory; Algorithms, 20h, Agrégation, ENS Rennes, France;

Master: Ocan Sankur, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;

Master: Ocan Sankur, *Travaux pratiques*, Analyse et Conception Formelle (ACF), 22h, M1, Univ Rennes 1, 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.

10.2.2. Supervision

- PhD: Matthieu Pichené, Multi-level analysis in computational system biology : the case of HeLa cells under apoptosis treatment [2], Univ. Rennes 1. The defense took place on June 25, 2018, and was supervised by Blaise Genest.
- PhD: Engel Lefaucheux, Controlling information in probabilistic systems [1], Univ. Rennes 1. The defence took place on September 24, 2018, and was supervised by Nathalie Bertrand and Serge Haddad (ENS Paris-Saclay).
- PhD in progress: Hugo Bazille, Information flows in quantitative dynamic systems, started oct. 2016, Blaise Genest and Éric Fabre.
- PhD in progress: Sihem Cherrared, Diagnosis of multi-tenant programmable networks, started Dec. 2016, Éric Fabre, Gregor Goessler (Inria, Spades) and Sofiane Imadali (Orange).
- PhD in progress: Emily Clement, Verification and synthesis of control systems: efficiency and robustnes, started Dec. 2018, supervised by Thierry Jéron, Nicolas Markey, and David Mentré (Mitsubishi Electric)
- PhD in progress: Rodrigue Djeumen Djatcha, Collaborative Model for Urban Crowdsourcing, University of Douala, Cameroon, supervised by Éric Badouel.
- PhD in progress: Erij Elmajed, Diagnosis of reconfigurable systems, started March 2017, Éric Fabre and Armen Aghasaryan (Nokia).
- PhD in progress: Léo Henry, Optimal test-case generation with game theory, started Oct. 2018, supervised by Thierry Jéron and Nicolas Markey.
- PhD in progress: Karim Kecir, Régulation et robustesse des systèmes ferroviaires urbains, defense planned on the 1st semester 2019, supervised by Loïc Hélouët and Pierre Dersin (Alstom).
- PhD in progress: Anirban Majumdar, Games for distributed networks: models and algorithms, ENS Paris Saclay, France, supervised by Nathalie Bertrand and Patricia Bouyer.
- PhD in progress: Rituraj Singh, Data-centric Workflows for Crowdsourcing Applications, defense planned on February 2021, supervised by Loïc Hélouët.
- PhD in progress: Robert Fondze Jr Nsaibirni, A Guarded Attribute Grammar Based Model for User Centered, Distributed, and Collaborative Case Management – Case of the Disease Surveillance Process, University of Yaoundé, Cameroon, supervised by Éric Badouel.
- PhD in progress: The Anh Pham, Dynamic Formal Verification of High Performance Runtimes and Applications, started Nov. 2016, supervised by Thierry Jéron and Martin Quinson (Myriads, Inria Rennes).
- PhD in progress: Arthur Queffelec, Tradeoff between Robustness and Optimality in Strategic Reasoning, started Nov. 2018, supervised by Ocan Sankur and François Schwarzentruber (Logica, Irisa).
- PhD in progress: Victor Roussanaly, Efficient verification of timed systems, started Sep. 2017, supervised by Nicolas Markey and Ocan Sankur.
- PhD in progress: Suman Sadhukhan, Modelling and parameterized verification of mobile networks, started Oct. 2018, supervised by Nathalie Bertrand, Nicolas Markey, Ocan Sankur.

10.2.2.1. Master Students

- Ocan Sankur co-supervised the master's thesis (M2) of Arthur Queffelec.
- Thierry Jéron and Nicolas Markey supervised the master's thesis (M2) of Léo Henry.
- Nathalie Bertrand, Loïc Hélouët and Ocan Sankur supervised a training period (3 h/week during 6 months) for a group of master 1 students. The topic was application of model checking to assess the performance of regulation algorithms.
- Loïc Hélouët supervised the internship of master student Flavia Palmieri.

10.2.2.2. Other Internships

- L3 Intership of Mélanie Bratulic, supervised by Sophie Pinchinat (Logica, Irisa) and Thierry Jéron.

10.2.3. Juries

10.2.3.1. PhD Defenses

- Loïc Hélouët was an examiner in the PhD defense of Yann Duplouy, Ecole Normale Supérieure Paris-Saclay, November 2018.
- Thierry Jéron was a reviewer for the PhD thesis of Antoine EL HOKAYEM, Univ. Grenoble, December 2018.
- Nicolas Markey was a reviewer for the PhD thesis of Benedikt Brütsch (Decembre 20, 2018, Aachen, Germany; PhD student of Wolfgang Thomas); a reviewer for the PhD thesis of Petr Bezděk (on March 9, 2018, Masaryk University, Brno, Czech Republic; PhD student of Ivana Černá); and a reviewer for the PhD thesis of Nicola Gigante (January 2019, Udine, Italy; PhD student of Angelo Montanari).
- Nathalie Bertrand was an examiner for the PhD thesis of Philipp Schlehuber-Caissier, Sorbonne Université, December, 14 2018; a reviewer for the PhD thesis of L'uboš Korenčiak, Masaryk University (Czech Republic), April 2018; and an examiner for the PhD thesis of Othmane Rezine, Uppsala University, January, 12 2018.

10.2.3.2. Other Juries

- Nathalie Bertrand was in the hiring committee for CRCN positions at Inria Rennes Bretagne Atlantique in 2018. She was also in the hiring committee for a Maitre de conférences position at Université Paris-Est Créteil in spring 2018.

10.2.4. Books

Nicolas Markey co-authored the chapter on *Model Checking Real-Time Systems* in the book *Handbook of Model Checking* [29].

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

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 DPEI (European and International Partnership Department). He is member of the executive board of GIS SARIMA.

10.3.2. Articles and contents

- Ocan Sankur published an article on formal verification for the Turkish Academy of Sciences: "How to verify computer systems on which our lives depend" on Nov. 2018.

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, 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 Lyon on June 25–29, 2018. 5 days / 8 lectures / 25 participants. https://ejcp2018.sciencesconf.org/

D. Gallois-Wong, co-chair of the Doctoral Programme of the 11th Conference on Intelligent Computer Mathematics (CICM 2018).

10.1.1.2. Member of the Organizing Committees

G. Melquiond, organizer of the 10th "Rencontres Arithmétiques du GDR Informatique-Mathématique" (RAIM 2018)

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

S. Boldo, program chair of the 29th "Journées Francophones des Langages Applicatifs" (JFLA 2018).

S. Boldo, program co-chair of the 26th IEEE Symposium on Computer Arithmetic (ARITH 2019), Kyoto, Japan.

10.1.2.2. Member of the Conference Program Committees

S. Boldo, PC of the 25th IEEE Symposium on Computer Arithmetic (ARITH 2018)

S. Boldo, PC of the 7th ACM SIGPLAN Conference on Certified Programs and Proofs (CPP 2018)

S. Boldo, PC of the Tenth NASA Formal Methods Symposium (NFM 2018)

S. Boldo, PC of the Eleventh NASA Formal Methods Symposium (NFM 2019)

J.-C. Filliâtre, PC of the 18th International Workshop on Automated Verification of Critical Systems (AVOCS 2018)

J.-C. Filliâtre, PC of the 10th International Conference on Interactive Theorem Proving (ITP 2019)

J.-C. Filliâtre, PC of the European Symposium on Programming (ESOP 2020)

J.-C. Filliâtre, PC of the Symposium on Languages, Applications and Technologies (SLATE 2018)

G. Melquiond, PC of the 26th IEEE Symposium on Computer Arithmetic (ARITH 2019)

G. Melquiond, PC of the 10th International Conference on Interactive Theorem Proving (ITP 2019)

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*.

J.-C. Filliâtre, member of the editorial board of *Journal of Functional Programming*.

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

J.-C. Filliâtre, invited speaker at the 8th International Conference on Interactive Theorem Proving (ITP 2018).

J.-C. Filliâtre, invited speaker at the Formal Integrated Development Environment (F-IDE 2018).

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).

J.-C. Filliâtre, chair of IFIP WG 1.9/2.15 verified Software.

10.1.6. Scientific Expertise

G. Melquiond, 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 (includes examination of proposals for creation of new Inria project-teams for Saclay research center).

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 the national Inria admission committee.

J.-C. Filliâtre, grading the entrance examination at X/ENS (*"option informatique"*).

C. Marché, scientific expert for project evaluation, Dutch Research Council (NWO https://www.nwo.nl/en), The Netherlands, 2018.

C. Marché, scientific expert for project evaluation, National Science Centre (Narodowe Centrum Nauki - NCN http://www.ncn.gov.pl/), Poland, 2018.

C. Marché, scientific expert for promotion of academic staff, Chalmers University of Technology, Sweden, 2018.

S. Boldo, member of a hiring committee for an associate professor position in computer science at University Paris Diderot (IRIF laboratory).

C. Marché, member of DigiCosme committee for research and innovation (selection of projects for working groups, post-doc grants, doctoral missions, invited professors)

10.1.7. Research Administration

G. Melquiond, member of the committee for the monitoring of PhD students (*"commission de suivi doctoral"*).

S Boldo, member of the CLFP (*"commission locale de formation permanente"*).

S. Boldo, member of the CCD, (*"commission consultative des doctorants"*).

S. Boldo will be deputy scientific director (DSA) of Inria Saclay research center from January 1st, 2019

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

J.-C. Filliâtre, *Langages de programmation et compilation*, 25h, L3, École Normale Supérieure, France.

J.-C. Filliâtre, *Les bases de l'algorithmique et de la programmation*, 15h, L3, École Polytechnique, France.

J.-C. Filliâtre, *Compilation*, 18h, M1, École Polytechnique, France.

G. Melquiond, *Programmation C++ avancée*, 12h, M2, Université Paris-Saclay, France.

10.2.2. Supervision

PhD: M. Clochard, “Methods and tools for specification and proof of difficult properties of sequential programs” [11], Université Paris-Saclay & Université Paris-Sud, March 30th 2018, supervised by C. Marché and A. Paskevich.

PhD: D. Declerck, “Verification via Model Checking of Parameterized Concurrent Programs on Weak Memory Models” [12], Université Paris-Saclay & Université Paris-Sud, Sep 24th 2018, supervised by F. Zaïdi (LRI) and S. Conchon.

PhD: M. Pereira, “Tools and Techniques for the Verification of Modular Stateful Code” [127], Université Paris-Saclay & Université Paris-Sud, Dec 10th 2018, supervised by by J.-C. Filliâtre.

PhD in progress: M. Roux, “Model Checking de systèmes paramétrés et temporisés”, since Sep. 2015, supervised by Sylvain Conchon.

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.

PhD in progress: Q. Garchery, “Certification de la génération et de la transformation d’obligations de preuve”, since Oct. 2018, supervised by C. Keller, C. Marché and A. Paskevich.

10.2.3. Juries

C. Marché: examiner of the habilitation thesis of J. Signoles, “From Static Analysis to Runtime Verification with Frama-C and E-ACSL”, Université Paris-Sud, July 9th 2018

C. Marché: examiner of the habilitation thesis of N. Kosmatov, “Combinations of Analysis Techniques for Sound and Efficient Software Verification”, Université Paris-Sud, Nov 20th 2018

C. Marché: president of the PhD defense of J.-C. Léchenet, “Certified Algorithms for Program Slicing”, Université Paris-Saclay, July 19th 2018

C. Marché: reviewer of the PhD defense of C. Laurenço, “Single-assignment Program Verification”, Universidad do Minho, Portugal, July 2nd 2018

S. Boldo: reviewer and president of the PhD defense of B. Djalal, “Formalisation en Coq pour la décision de problèmes en géométrie algébrique réelle”, Université Côte d’Azur, December 3rd 2018

S. Boldo: reviewer of the PhD of R. Picot, “Amélioration de la fiabilité numérique de codes de calcul industriels”, Sorbonne Université, March 27th 2018

S. Boldo: president of the PhD defense of S. Covanov, “Algorithmes de multiplication : complexité bilinéaire et méthodes asymptotiquement rapides”, Université de Lorraine, June 5th 2018

S. Boldo: president of the PhD defense of G. Davy, “Génération de codes et d’annotations prouvables d’algorithmes de points intérieurs à destination de systèmes embarqués critiques”, Université de Toulouse, December 6th 2018

J.-C. Filliâtre: licentiate doctorate examination at Chalmers University of Technology, Sweden, August 23, 2018.

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

S. Boldo is the scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.

She was also responsible (with M. Quet of the SCM) for the 2018 “Fête de la science” on October 11th 2018. About 260 teenagers were welcomed on 8 activities ranging from unplugged activities with Duplo construction toys to programming, and from applied mathematics to theoretical computer science.

10.3.2. Interventions

S. Boldo animated an activity at the Inria “Fête de la science” on October 11th 2018 the whole day long.

S. Boldo animated an activity and gave talks at the LRI “Fête de la science” on October 12th 2018.

S. Boldo gave a talk during at a *Girls can code* week on August 31st 2018 in Paris.

S. Boldo will give a talk to about 180 teenagers at the Marie Curie high school in Sceaux on February 8th, 2019

J.-C. Filliâtre gave a talk at *Mathematical Summer in Paris* on July 16, 2018.

J.-C. Filliâtre gave a talk *Parcours d’un informaticien* at the seminar *“Info Pour Tous”* (high school and undergraduate students). Video on YouTube. http://seminairespourtous.ens.fr/ipt

S. Dailler and C. Marché gave a demonstration of the SPARK environment, at the DigiHall Day (May 22 2018 https://www.irt-systemx.fr/evenements/digihall-2018/). DigiHall is a cluster of digital technologies of Paris-Saclay. More than 800 industrial and institutional decision-makers and academic counterparts took part in this first-of-its-kind event.

C. Marché presented the joint laboratory ProofInUse at the LabCom Colloquium (Maison de la Chimie, Paris, Sep. 27 2018 http://ptolemee.com/colloque-labcom/index.html) organized by ANR, with participation of numerous actors from both academia and industry.

10.3.3. Internal action

S. Boldo demonstrated popularization by an unplugged activity to all the new Inria staff at the welcome days on June 7th 2018

S. Boldo animated an unplugged activity to the AER service (team assistants) on July 3rd 2018

S. Boldo trained colleagues on unplugged activities for the “Fête de la science” (5 sessions of about 1h30)

S. Dailler and C. Marché gave a presentation of the joint laboratory ProofInUse, together with a demonstration of the SPARK environment, at the Software Day of the DigiCosme Labex (Saclay, June 7 2018 https://digicosme.lri.fr/tiki-read_article.php?articleId=256)

10.3.4. Creation of media or tools for science outreach

S. Boldo is supervising the popularization mission of C. Patte (M3DISIM team) in order to create a new popularization activity for teenagers in 2019.

C. Marché, main contributor of the site for the Why3 tool inside the Inria Saclay Virtual Showroom. Includes a short video introduction of Why3 for beginners using the TryWhy3 Web interface http://why3.lri.fr/try/

VERIDIS Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Organization of Scientific Events

Jasmin Blanchette co-organized the first *Verification and Deduction Mentoring Workshop* (VDMW 2018) as part of the Federated Logic Conferences (FLoC 2018) in Oxford, UK. He also coorganized two workshops at VU Amsterdam: the First European Workshop on *Higher-Order Automated Reasoning* (Matryoshka 2018) and the Fourth International *Workshop on Automated (Co)inductive Theorem Proving* (WAIT 2018).

Igor Konnov and Stephan Merz were organizers of the fifth *Workshop on Formal Reasoning in Distributed Algorithms* (FRIDA 2018) as part of the Federated Logic Conference (FLoC 2018) in Oxford, UK.

Stephan Merz was the main organizer of the TLA$^+$ Community Meeting as part of the Federated Logic Conference (FLoC 2018) in Oxford, UK.

Thomas Sturm co-organized two international interdisciplinary workshops on *Symbolic Methods for Biological Networks* at the University of Bonn, Germany.

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 2018, VTSA took place in August in Nancy, France.

9.1.2. Program Committees

9.1.2.1. Chair of Conference Program Committees

Igor Konnov served as a chair of the *Artifact Evaluation Committee* at *Computer-Aided Verification* (CAV 2018).

Dominique Méry was a co-chair of the program committee of the 8th International Conference on Model and Data Engineering (MEDI 2018), organized in Marrakesh, Morocco, in October 2018.

Uwe Waldmann co-chaired the program committee of Deduktionstreffen 2018, the annual meeting of the Interest Group for Deduction Systems (FGDedSys) of the AI Chapter of the German Society of Informatics.

9.1.2.2. Member of Conference Program Committees

Jasmin Blanchette served on the program committees of the *NASA Formal Methods* Symposium (NFM 2018), the Conference on *Computer-Aided Verification* (CAV 2018), the *International Conference on Tests and Proofs* (TAP 2018), the *International Joint Confrence on Automated Reasoning* (IJCAR 2018), the Interational Conferene on *Interactive Theorem Proving* (ITP 2018), the ACM SIGPLAN International Conference on *Certified Programs and Proofs* (CPP 2018), and the Conference on *Artificial Intelligence and Theorem Proving* (AITP 2018). He also served on the workshop committees for the *International Workshop on the Implementation of Logics* (IWIL 2018) and the *Deduktionstreffen* 2018.

Pascal Fontaine served on the program committees of the *International Joint Confrence on Automated Reasoning* (IJCAR 2018), the *International Workshop on the Implementation of Logics* (IWIL 2018), the *International Workshop on Practical Aspects of Automated Reasoning* (PAAR 2018), the *Satisfiability Checking and Symbolic Computation* Workshop (SC-Square 2018).

Igor Konnov served on the program committees of *ACM Symposium on Principles of Distributed Computing* (PODC 2018), *Formal Methods in Computer-Aided Design* (FMCAD 2018), *International Conference on Verification and Evaluation of Computer and Communication Systems* (VECoS 2018), *International Symposium on Formal Approaches to Parallel and Distributed Systems* (4PAD 2018), *Workshop on Methods and Tools for Rigorous System Design* (MeTRiD 2018), and *Workshop on Program Semantics, Specification, and Verification* (PSSV 2018).

Dominique Méry served on the program committees of the *International Conference on Engineering of Complex Computer Systems* (ICECCS 2018), the *International Symposium on Formal Methods* (FM 2018), the *International Conference on Formal Engineering Methods* (ICFEM 2018), the *International Conference on Integrated Formal Methods* (iFM 2018), the *International Conference on ASM, Alloy, B, TLA, VDM and Z* (ABZ 2018), the *Workshop on Formal Methods for Interactive Systems* (FMIS 2018), the *Workshop in Formal Models for Mastering Multifaceted Systems* (REMEDY 2018), the *Workshop on Formal Approaches for Advanced Computing Systems* (FAACS 2018), and the *Workshop on Software Engineering in Healthcare Systems* (SEHS 2018).

Stephan Merz served on the program committees of the *International Conference on ASM, Alloy, B, TLA, VDM and Z* (ABZ), the *International Conference on Formal Methods for Industrial Critical Systems* (FMICS), the *International Conference on Formal Engineering Methods* (ICFEM), the *International Symposium on Dependable Software Engineering: Theories, Tools, and Applications* (SETTA), the *International Workshop on Automated Verification of Critical Systems* (AVoCS), and the *International Workshop about Sets and Tools* (SETS).

Sorin Stratulat served on the program committees of the *International Symposium on Symbolic and Numeric Algorithms for Scientific Computing* (SYNASC 2018), the *International Conference on Information Assurance and Security* (IAS 2018), and the *International Conference on Computational Intelligence in Security for Information Systems* (CISIS 2018).

Thomas Sturm served on the program committees of *Automated Deduction in Geometry* (ADG 2018), *Computer Algebra in Scientific Computation* (CASC 2018), the *International Joint Confrence on Automated Reasoning* (IJCAR 2018), the *Satisfiability Modulo Theories* Workshop (SMT 2018), the *Satisfiability Checking and Symbolic Computation* Workshop (SC-Square 2018).

Uwe Waldmann served on the program committee of the *International Joint Confrence on Automated Reasoning* (IJCAR 2018).

Christoph Weidenbach served on the program committee of the *International Joint Conference on Automated Reasoning* (IJCAR 2018) and the senior program committee of *International Joint Conference on Artificial Intelligence* (IJCAI 2018).

9.1.3. Journals

9.1.3.1. Member of Editorial Boards

Jasmin Blanchette and Stephan Merz served as guest editors for the special issue on *Interactive Theorem Proving* (ITP 2016) of the *Journal of Automated Reasoning*.

Dominique Méry is Book Reviews Editor for *Formal Aspects of Computing*.

Thomas Sturm is an editor of the *Journal of Symbolic Computation* (Elsevier) since 2003 and an editor of *Mathematics in Computer Science* (Springer) since 2013.

Christoph Weidenbach is a member of the editorial board of the *Journal of Automated Reasoning* (Springer). He also served as an editor on the special issue on *Automated Reasoning Systems* of JAR.

9.1.4. Invited Talks

Jasmin Blanchette was invited to give a seminar talk at the University of Edinburgh on the IsaFoL (Isabelle Formalization of Logic) project.

Marie Duflot-Kremer was an invited speaker at EduCode 2018 in Brussels, Belgium, where she presented the Class'Code project.

Pascal Fontaine was an invited speaker at Deduktionstreffen 2018 in Luxembourg. He was an invited lecturer at the EPIT 2018 Software Verification Spring School in Aussois, France and at the SAT-SMT-AR school 2018 in Manchester, UK.

Igor Konnov was invited to give a tutorial at the Dagstuhl Seminar 18211 "Formal Methods and Fault-Tolerant Distributed Computing: Forging an Alliance" in Dagstuhl, Germany. He was also invited to give talks at the Workshop on Verification of Distributed Systems, Essaouira, Morocco, and Helmut Veith Memorial Workshop in Obertauern, Austria. Furthermore, he gave a talk (together with Josef Widder) on one of the research highlights of the RISE project at Alpine Verification Meeting in Wagrain, Austria.

Stephan Merz was invited to give a seminar talk at EPFL Lausanne on the use of auxiliary variables for proving refinement between TLA$^+$ specifications.

Thomas Sturm was an invited speaker at ISSAC 2018 in New York. He was furthermore invited to give a lecture at the graduate school for mathematics at RWTH Aachen University, Germany, and a seminar talk at Johannes Kepler University Linz, Austria.

Uwe Waldmann was invited to give a tutorial on Saturation Theorem Proving at the SAT/SMT/AR Summer School 2018 in Manchester, UK.

Christoph Weidenbach gave an invited talk on Robust Automated Reasoning at the 2018 Innsbruck Symposium on Integration of Automated Deduction and Interactive Theorem Proving.

9.1.5. Leadership within the Scientific Community

Jasmin Blanchette is a regular member of the CADE (*Conference on Automated Deduction*) Inc. Board of Trustees. He is also a regular member of the steering committees for the ITP (*Interactive Theorem Proving*) and TAP (*Tests and Proofs*) conference series.

Marie Duflot-Kremer is an elected member of the council of SIF, the French association for computer science.

Pascal Fontaine is an SMT-LIB manager, together with Clark Barrett (Stanford University) and Cesare Tinelli (University of Iowa). He is a regular member of steering committees for the FroCoS (*Frontiers of Combining Systems*) conference series, and for the SC-Square (*Satisfiability Checking and Symbolic Computation* workshop series. He is ex-officio member of the CADE (*Conference on Automated Deduction*) Inc. Board of Trustees. He is an elected member of the steering committee for the SMT (*Satisfiability Modulo Theories*) workshop series.

Stephan Merz is a member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*, a member of the committee for the SIF thesis award (*Prix Gilles Kahn*), and a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS).

Thomas Sturm is a member at large of the steering committee of the ACM 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.

9.1.6. Scientific Expertise

Dominique Méry and Stephan Merz served as experts for ANR, the French national research agency.

Christoph Weidenbach served as an expert for the German Science Foundation (DFG).

9.1.7. Research Administration

Marie Duflot-Kremer is an elected member of the council of LORIA. She was a member of the hiring committee for an associate professor at Université Paris-Est-Créteil.

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 2018, he was a member of the hiring committees of senior researchers at Inria and of junior researchers at Inria Paris. He is also a member of the *bureau* of the computer science committee of the doctoral school IAEM Lorraine and of the executive committee of the project on citizens' trust in the digital world (DigiTrust) funded by *Lorraine Université d'Excellence*.

Uwe Waldmann is a member of the admissions committee for scholarships of the International Max-Planck Research School for students aiming at a master's degree.

Christoph Weidenbach is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

9.2. Teaching, Supervision, PhD Committees

9.2.1. Teaching

Licence: Marie Duflot-Kremer is the head of the first year for computer science students at the Faculty for Science and Technology of Université de Lorraine.

Licence: Marie Duflot-Kremer, Algorithmique et Programmation 1, 60 HETD L1 Mathématiques, Informatiques, Sciences pour l'Ingénieur, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Introduction au Web, 30 HETD L1 Mathématiques, Informatiques, Sciences pour l'Ingénieur, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Méthodologie du Travail Universitaire, 24 HETD, L1 Informatique, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Bases de données 2, 20 HETD, L2 Informatique, Université de Lorraine, France.

Licence: Marie Duflot-Kremer, Programmation Web, 10 HETD, L3 Informatique, Université de Lorraine, France.

Licence: Pascal Fontaine, Structure des ordinateurs, 47 HETD, L2 MIASHS, parcours MIAGE, Université de Lorraine, France.

Licence: Sorin Stratulat, Bases de données, 32 HETD, L1, ISFATES, France.

Master: Jasmin Blanchette, Logical Verification, 36 HETD, M1/M2, Vrije Universiteit Amsterdam, the Netherlands.

Master: Marie Duflot-Kremer, Vérification de systèmes, 30 HETD, M1 Informatique, Université de Lorraine, France.

Master: Marie Duflot-Kremer and Stephan Merz, Elements of model checking, 40 HETD, M2 Informatique and Master Erasmus Mundus DESEM, Université de Lorraine, France.

Master: Marie Duflot-Kremer and Stephan Merz, Conception et architectures distribuées, 24 HETD M1 informatique, Université de Lorraine, France.

Master: Pascal Fontaine, Réseaux, 50 HETD, M1 MIAGE, Université de Lorraine, France.

Master: Pascal Fontaine is the head of the MIAGE degree at Université de Lorraine.

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: Sorin Stratulat, Analyse et conception de logiciels, 105.5 HETD, M1 Informatique, Université de Lorraine, France.

Master: Sorin Stratulat, Génie Logiciel, 30 HETD, M2 Informatique, Université de Lorraine, France.

Master: Uwe Waldmann, Automated Reasoning I, 90 HETD, Universität des Saarlandes, Germany.

Master: Sophie Tourret and Uwe Waldmann, Automated Reasoning II, 60 HETD, Universität des Saarlandes, Germany.

9.2.2. Supervision

HdR: Pascal Fontaine, Satisfiability Modulo Theories, Université de Lorraine, 8 October 2018.

PhD: Souad Kherroubi, Un cadre formel pour l'intégration de connaissances du domaine dans la conception des systèmes: Application au formalisme Event-B, Université de Lorraine, 21 December 2018. Supervised by Dominique Méry.

PhD: Andreas Teucke, *An Approximation and Refinement Approach to First-Order Automated Reasoning*, Saarland University. Supervised by Christoph Weidenbach, defended in May 2018.

PhD in progress: Martin Bromberger, Arithmetic Reasoning, Saarland University. Supervised by Thomas Sturm and 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: Alexis Grall, Integration of a modeling language and a language for programming distributed systems, Université de Lorraine. Supervised by Horatiu Cirstea and Dominique Méry, since October 2018.

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 Thomas Sturm and Christoph Weidenbach, since November 2013.

Jasmin Blanchette supervises two PhD students at VU Amsterdam and was a supervisor of Anders Schlichtkrull at TU Denmark, who defended in 2018. Igor Konnov co-supervises three PhD students at TU Wien. These PhD students are not members of VeriDis.

9.2.3. Thesis committees

Pascal Fontaine served as a reviewer in the thesis committees for Ahmed Irfan at Fondazione Bruno Kessler and University of Trento, Italy, for Vu Xuan Tung at JAIST, Japan, and for Mêton Mêton Atindehou at Université Catholique de Louvain (UCL), Belgium.

Stephan Merz served as a reviewer for the PhD theses of Bin Fang (Univ. Paris Diderot and East China Normal University) and Hai Nguyen Van (Univ. Paris Saclay). He was an examiner for the PhD committees of Evgeny Kotelnikov (Chalmers Univ.) and for the habilitation thesis of Nikolai Kosmatov (CEA Saclay).

Thomas Sturm served as a reviewer in the thesis committee for Ulrich Loup at RWTH Aachen University, Germany.

9.3. Popularization

9.3.1. Articles and Contents

In addition to the creation of unplugged computer science activities, Marie Duflot-Kremer produces documents to help others, together with videos already produced in collaboration with Inria, master and practise on their own those activities.

An article was accepted at the Educode conference on the analysis of unplugged vs. computer based programming learning [32].

9.3.2. Education

Marie Duflot-Kremer is involved in various training activities for high school teachers. She is involved in two IREM (Institute for Research on Mathematics Education) groups that produced a training session, she gave workshops in the regional APMEP (Association of Math Teachers from Public Education) day and during the "Journée ISN" (organized for teachers involved in computer science courses in high school). She also gave a conference talk and a workshop on a one day training session for teachers at the Science Museum "Le Vaisseau" in Strasbourg.

Thomas Sturm and Christoph Weidenbach co-organized the scientific track of the training program of the German team for the International Olympiad in Informatics (IOI).

9.3.3. Interventions

Marie Duflot-Kremer is involved in many outreach events where computer science is shared with a very wide audience, from 3 to 80+ years old, including "Journée des cordées de la réussite" and "Journée d'immersion" (for high school students), Fête de La Science (locally and in Paris with Inria including a theater play performed at Cité des Sciences), Math en Jeans (a program where high school students discover research through simple mathematics or computer science problems).

She gave a two-day seminar at Université Paris Nanterre to Law teachers presenting computer networks and computer security, and a talk at the "Journée GDR IA" to show to AI researchers how to present their research to a wide audience through unplugged activities.

Marie Duflot-Kremer was also one of the trainers at a three-day summer school on computer science outreach held by Société Informatique de France. During these three days the trainees discovered the concept, practised existing activities and even created their own (on subject as diverse as information leakage, Turing machines or binary integer encoding).

Concerning events organized by Inria, she took part in the Ada Lovelace Day organized by Inria Nancy – Grand Est (NGE), on three aspects: organization of the day (both scientific and practical), training of colleagues prior to the event, and supervising workshops during the event. She is also part of the FAN (Formation des Ambassadeurs du Numérique) project organised by Inria NGE and "Les Petits Débrouillards" that will, in addition to the Class'Code MOOC, train people involved in education (in school or outside) through 5 days of training seminar. She also took part in two events related to Class'Code in Bordeaux (May) and Poitiers (November), introducing the motivations of unplugged activities and their practical aspects in workshops.

9.3.4. Internal Action

Marie Duflot-Kremer is part of the "Info Sans Ordi" group affiliated to Société Informatique de France, where people share and design new unplugged activities to introduce computer science concepts.

9.3.5. Creation of Media or Tools for Science Outreach

Marie Duflot-Kremer and the Inria media team recorded three new videos presenting unplugged activities, that complement the 10 videos already existing and available on the Pixees Youtube account. She is a member of the GT7F working group (led by Interstice/Inria) that has produced a card game presenting important computer science figures (to be released in early 2019).

CIDRE Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

Jean-Louis Lanet served as general chair of the 13rd International Conference on Risks and Security of Internet and Systems CRiSIS 2018, Bordeaux France and general chair of the 11th International Conference on Information Technology and Communication Security, Bucharest, Romania,

9.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2018 (25rd Computers & Electronics Security Applications Rendez-vous), November 2018, Rennes, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2018 (Symposium sur la sécurité des technologies de l'information et des communications) that took place in Rennes, France in June, where it gathered more than 600 participants.

Gilles Guette served as a member of the organization committee of InOut18, annual event on new mobility that took place in Rennes, France in March.

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

Eric Totel chaired the Program Committee of the 2018 French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

9.1.2.2. Member of the Conference Program Committees

Frédéric Tronel and Valérie Viet Triem Tong served as a member of the program committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) June 2018, Rennes, France.

Valérie Viet Triem Tong served as a member of the program committee of SECITC (International conference on Information Technology and Communications Security), october 2018, Bucharest, Romania.

Jean-François Lalande served as a member of the program committee of the international conferences CECC 2018, IEEE AINS 2018, IEEE HPCS 2018 and of the international workshops SHPCS 2018, IWCC 2018, CUING 2018, BioSTAR 2018, WTMC 2018, DACSW 2018.

Michel Hurfin acts as a member of the program committee of the African Conference on Research in Computer Science and Applied Mathematics (CARI 2018), South Africa, October 2018.

Emmanuelle Anceaume served as a member of the program committee of the following international conferences: ICDCN 2018, NCA 2018 CryBlock 2018, DEBS 2018, PEC 2018, BSCT 2018, and ADSN 2018.

Ludovic Mé served as a member of the 2018 MSPN (International Conference on Mobile, Secure and Programmable Networking) and CARI (Colloque Africain sur la Recherche en Informatique et Mathématiques Appliquées 2018) program Committees.

Guillaume Piolle served as a member of the 2018 APVP (Atelier sur la Protection de la Vie Privée) and EGC-IA (Extraction et Gestion des Connaissances - Intelligence Artificielle) program committees.

Gilles Guette served as a member of the program committee of the International Conference on Information Systems Security and Privacy, ICISSP 2018.

9.1.2.3. Reviewer

Valérie Viet Triem Tong served as a reviewer for the African Conference on Research in Computer Science and Applied Mathematics, October 2018, South Africa, Stellenbosch.

Jean-François Lalande served as a reviewer for ICISSP 2018, APVP 2018.

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

Jean-François Lalande served as a member of the editorial board of IARIA International Journal on Advances in Security.

Michel Hurfin serves as a member of the editorial board of the JISA Journal (Journal of Internet Services and Applications - Springer).

9.1.3.2. Reviewer - Reviewing Activities

Jean-François Lalande served as a reviewer for Journal of Universal Computer Science, Elsevier FGCS, IEEE TIFS, MDPI Future Internet, MDPI Sensors, Elsevier Computer Commmunications.

Michel Hurfin served as a reviewer for the IEEE TDSC Journal (Transactions on Dependable and Secure Computing), the Springer TOCS Journal (Theory of Computing Systems), and the Taylor & Francis International Journal of Control.

Emmanuelle Anceaume served as a reviewer of the following journals: IEEE TPDS, and ACM TAAS.

Jean Louis Lanet served as reviewer for the Journal of Computer Security.

Guillaume Piolle served as a reviewer for the RIA (Revue d'Intelligence Artificielle) journal.

Guillaume Hiet served as a reviewer for the Journal of Computer Security.

Gilles Guette served as a reviewer for the IEEE JSAC-SI-NETSOFT-ENABLERS and for the IEEE Networking Letters.

9.1.4. Invited Talks

Emmanuelle Anceaume gave several talks:

- *UTXOs as a proof of membership for Byzantine Agreement based Cryptocurrencies* during the National Days of the pre-GDR on security, june 2018.
- *Beyond the block: A lego blockumentary* during “Journées scientifiques de l'Inria”.
- *Sycomore, a Directed Acyclic Graph of Blocks*, Chain-in conference, Porto, Portugal, July 2018, [6], also on Youtube “https://www.youtube.com/watch?v=YLW-iHjsWo0”.

Valérie Viet Triem Tong gives a talk about *information flow monitoring at the operating system level* during the National Days of the pre-GDR on security, june 2018.

Jean-François Lalande was invited as keynote speaker at SecITC'2018 [7].

Jean-François Lalande was an invited speaker of the workshop SHPCS 2018 [8].

Guillaume Piolle was an invited speaker at the *Surveillance Resilience, & Privacy* conference (Paris, December 2018).

9.1.5. Scientific Expertise

Ludovic Mé has served the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).

Ludovic Mé has chaired the group of experts dedicated to the evaluation of the security of French computer science research labs (PPST S/C 7).

Ludovic Mé has chaired 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).

Eric Totel has served 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).

Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR).

9.1.6. Research Administration

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 was the president of a recruitment committee for an assistant professor position at the CNAM (Conservatoire national des arts et métier, Paris). He also served a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.

Valérie Viet Triem Tong was a member of a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.

9.2. Teaching - Supervision - Juries

9.2.1. 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*, 36 hours, L1 - Licence, ISTIC/University of Rennes, France;

Licence: Gilles Guette, *Network Initiation*, 72 hours, L3 - Licence, ISTIC/University of Rennes, France;

Licence: Gilles Guette, *Network Initiation*, 69 hours, L3 - first year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Routing*, 45 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*, 13 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*, 46 hours, M1 - second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Sensors Network*, 28 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;

Licence: Jean-François Lalande, *Algorithms and data structures*, 22 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Computer Sciences*, 13 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Operating System*, 7 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Legal aspects of information security*, 4 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Android mobile development*, 18 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Web development*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Jean-François Lalande, *Supervision of student projects*, 7 projects, 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, *Operating systems*, 21 hours 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*, 2 projects of 2nd year of the engineer degree, CentraleSupélec, France;

Master: Valérie Viet Triem Tong is responsible of the M2 degree in *CyberSecurity* (mastère spécialisé), organized jointly by CentraleSupélec and Institut Mines Télécom (IMT) Atlantique, 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, , *Compilers*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Valérie Viet Triem Tong, *Supervision of student project*, 2 project, mastere CS (Cyber Security), CentraleSupélec, France;

Master : Valérie Viet Triem Tong, *Supervision of student project,* 1 project, M2 - third year of the engineer degree, CentraleSupélec, France;

Doctorant : Valérie Viet Triem Tong, *Malware analysis*, 6 hours, Research week, ENS Lyon, Lyon, France;

9.2.2. Supervision

9.2.2.1. Thesis defended in 2018

PhD: Thomas Letan, *Contribution à la sécurité des couches basses des systèmes d'information*, novembre 2018, supervised by Guillaume Hiet (50%), Pierre Chifflier (25% - ANSSI), and Ludovic Mé (25%);

PhD: Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, november 2018, supervised by Stéphane Mocanu (50% - Gipsa-lab), Guillaume Hiet (25%), and Jean-Marc Thiriet (25% - Gipsa-lab);

PhD : Mourad Leslous, *Highlighting and executing Android suspicious execution path in Android malware*, 18th december 2018, supervised by Thomas Genet (20% - Celtique Inria project), Jean François Lalande (40% - INSA Centre Val de Loire), and Valérie Viet Triem Tong (40%);

PhD : Yves Mocquard, *Population protocols*, december 2018, supervised by Bruno Sericola (Dyonisos Inria project) and Emmanuelle Anceaume;

PhD : Razika Lounas, *Validation des spécifications formelles de la mise à jour dynamique des applications Java Card*, December 2018, supervised by Jean-Louis Lanet (50%) and Mohamed Mezguiche (50%-Limose, Algerie)

PhD : Abdelhak Mesbah, *Rétroconeption d'application Java Card*, November 2018, supervised by Jean-Louis Lanet (50%) and Mohamed Mezguiche (50%-Limose, Algerie)

9.2.2.2. Theses in progress

PhD in progress (previously in Tamis): Aurélien Palisse, *Detection and early mitigation of ransomware on Windows platforms*, started in 2015, supervised by Jean-Louis Lanet and Hélène Le Bouder (IMT Atlantique);

PhD in progress (previously in Tamis): Kevin Bukasa, *Vulnerability analysis of a Secure Enclave in Embedded Devices*, started in 2016, supervised by Jean-Louis Lanet and Ronan Lashermes (SED Inria);

PhD in progress (previously in Tamis): Leopold Ouairy, *Analyse des vulnérabilités dans des systèmes embarqués*, started in 2017, supervised by Jean-Louis Lanet;

PhD in progress: Mathieu Escouteloup *Micro-architectures Sécurisées*, started in 2018, supervised by Jean-Louis Lanet and Jacques Fournier (CEA);

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: 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 : 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).

PhD in progress : Cedric Herzog, *Simulation d'environnement d'observation afin d'éviter le déploiement de malware sur une station de travail*, started in November 2018, supervised by Jean Louis Lanet (50%), Pierre Wilke (25%) and Valérie Viet Triem Tong (25%);

PhD in progress : Benoit Fournier, *Secure routing in drone swarms*, started in november 2018, supervised by Gilles Guette (50%), Jean Louis Lanet (25%) and Valérie Viet Triem Tong (25%);

PhD in progress : Aimad Berady, *Attacker characterization*, started in november 2018, supervised by Christophe Bidan (25%), Guillaume Carat (25%),Gilles Guette (25%), and Valérie Viet Triem Tong (25%);

PhD in progress : Cyprien Gottstein, *Problématiques de stockage et d'interrogation de très grands graphes répartis dans le contexte de l'internet des objets*, started in october 2018, supervised by Michel Hurfin (50%) and Philippe Raipin Parvedy (50%);

9.2.2.3. 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%);

Ruta Moussaileb, in progress, *From Data Signature to Behavior Analysis* started January 2018, supervised by Nora Cuppens (50%-) and Jean-Louis Lanet (50%)

9.2.3. Juries

Valérie Viet Triem Tong has reported the following PhD thesis:

Mickael Salaun, *Inte´gration de l'utilisateur au contro^le d'acce`s: du processus cloisonne´ a` l'interface homme-machine de confiance*, february 2018.

Alicia Filipiak, *Design and formal analysis of security protocols, an application to electronic voting and mobile payment*, march 2018.

Anaël Beaugnon, *Expert-in-the-Loop Supervised Learning for Computer Security Detection Systems*, june 2018.

Steve Muller, *Risk Monitoring and Intrusion Detection for Industrial Control System*, june 2018

Guilia De Santis, *Modeling and Recognizing Network Scanning Activities with Finite Mixture Models and Hidden Markov Models*, december 2018.

Jean-Louis Lanet has reported the following PhD thesis:

Mark Angoustures, December 2018, *Automatic malicious behaviors extraction usable in malware detection*

Damien Marion, December 2018 *Multidimensionality of the Models and the Data in the Side Channel Domain*

Guillaume Hiet was a member of the PhD committee for the following PhD thesis:

Thomas Letan, *Specifying and Verifying Hardware-based Security Enforcement Mechanisms*, October 2018.

Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, November 2018.

Muhammad Abdul WAHAB, *Support matériel pour l'analyse de sécurité du comportement des applications*, December 2018.

Valérie Viet Triem Tong was a member of the PhD committee for the following PhD thesis:

Guillaume Brogi, *Real-time detection of Advanced Persistent Threats using Information Flow Tracking and Hidden Markov Models*, february 2018.

Mourad Leslous, *Highlighting and Executing Suspicious Paths in Android Malwar*, december 2018.

Mark Angoustures, *Extraction automatique de caracte´ristiques malveillantes et me´thode de de´tection de malware dans un environnement re´el*, december 2018.

Jean-François Lalande has reported the following PhD thesis:

Guillaume Brogi, *Détection temps réel de Menaces Persistentes Avancées par Suivi de Flux d'Information et Modèles de Markov Cachés*, april 2018.

Jean-François Lalande was a member of the PhD committee for the following PhD thesis:

Mourad Leslous, *Highlighting and Executing Suspicious Paths in Android Malwar*, december 2018.

Jean-Louis Lanet was a member of the PhD committee for the following PhD thesis:

Khanh Huu The DAM, 2018, *Automatic Learning and Extraction of Malicious Behaviors*

Emmanuelle Anceaume was a member of the grading PhD committee of

Ivan Walulya PhD thesis *On design and applicatins of practical concurrent data structures*, Chalmers University, Sweden, November 2018.

Emmanuelle Anceaume was a member of the PhD committee of

Yves Mocquard, *Analyse probabiliste de protocoles de population* December, 2018.

Ludovic Mé was a member of the PhD committee for the following PhD committee of :

Tan Ngoc Nguyen, *A Security Monitoring Plane for Information Centric Networking: application to Named Data Networking*, Université de Technologie de Troyes, 2018.

9.3. Popularization

9.3.1. Articles and contents

- Emmanuelle Anceaume was interviewed by Jean-Michel Prima. This gave rise to an article: "Améliorer le Bitcoin ... à coup de fourches", Emergences Inria, 2018.
- Jean François Lalande and Valérie Viet Triem Tong were interviewed by Jean-Michel Prima. This gave rise to an article: "Disséquer automatiquement les malware sous Android", Emergences Inria, 2018.
- Emmanuelle Anceaume belonged to the working group “Blockchains challenges” organized by the french governmental group “France Strategie”. This gave rise to a report accessible here: https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf.

9.3.2. Interventions

Interviews, videos and podcasts :

Emmanuelle Anceaume was interviewed by Joanna Jongwane for a https://interstices.info/le-potentiel-revolutionnaire-de-la-technologie-blockchain/podcast in online Interstice journal, 2018. (Talk is in french).

Emmanuelle Anceaume was interviewed by the Parliamentary Office For Scientific and Technological Assessment (OPECST) in 2018. The OPECST acts as an intermediary between the political world and the world of research. The goal of this interview was to describe the Bitcoin cryptocurrency system and its associated blockchain, and to discuss on the different vulnerabilities Bitcoin is confronted with.

Emmanuelle Anceaume was interviewed by the *mission d’information sur l’usage des blockchains*, by the French National Assembly in 2018.

Demos : Practical results concerning malware analysis issued from the Kharon project were presented during:

Forum International de la Cybersécurité at Lille in 2018

Fête de la science at Inria in 2018

These works also regularly presented during the visits of the *Laboratoire Haute Sécurité* in the Inria Rennes Bretagne Atlantique center.

9.3.3. Internal action

- Emmanuelle Anceaume was invited to join the internal meetings at La Cordée Rennes on “Blockchain focus: Cinéma: Quel potential d’innovation”, November the 8th, 2018.

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 Steering Committee of CONCUR, the International Conference in Concurrency Theory. Since 2016.

The Organizing Committee of LICS, the ACM/IEEE Symposium on Logic in Computer Science. 2014-18.

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 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. Since 2005.

Frank D. Valencia is member of:

The steering committee of the International Workshop in Concurrency EXPRESS. Since 2010.

Konstantinos Chatzikokolakis is member of:

The steering committee of the Privacy Enhancing Technologies Symposium. Since 2018.

8.1.2. Scientific events selection committee

8.1.2.1. Chair of conference program committee

Konstantinos Chatzikokolakis:

is serving as PC chair (with Carmela Troncoso as co-chair) of PETS 2019: The 19th Privacy Enhancing Technologies Symposium, July 16-20, 2019, Stockholm, Sweden.

8.1.2.2. 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. Stockholm, Sweden, 16–20 July, 2019.

LICS 2019. The Thirty-Fourth Annual ACM/IEEE Symposium on Logic in Computer Science. Vancouver, Canada, 24–27 June 2019.

CSF 2019. The 32nd IEEE Computer Security Foundations Symposium. Hoboken, NJ, USA, June 24-27, 2019.

SAC 2019 (Security track). The 34th ACM/SIGAPP Symposium On Applied Computing. Limassol, Cyprus, 8-12 April 2019.

FACS 2018. The 15th International Conference on Formal Aspects of Component Software. Pohang, South Corea, 10-12 October 2018.

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.

PPML 2018. Privacy Preserving Machine Learning (NeurIPS 2018 Workshop). Montréal, Canada, 8 December 2018.

APVP 2018. Atelier sur la Protection de la Vie Privée. Porquerolles, France, 3-6 juin 2018.

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

Frank D. Valencia is/has been a member of the program committees of the following conferences and workshops:

CP-ICLP-SAT-DP-18. Doctoral Program of the 23rd International Conference on Principles and Practice of Constraint Programming.

CONCUR 2019. The 30th International Conference on Concurrency Theory. Amsterdam, the Netherlands, August 26-31, 2019.

AAMAS 2019. International Conference on Autonomous Agents and Multiagent Systems. Montreal, Canada, 13th-17th of May 2019.

8.1.3. Journals

8.1.3.1. Member of the editorial board

Catuscia Palamidessi is:

Member of the Editorial Board of the Proceedings on Privacy Enhancing Technologies (PoPETs), published by De Gruyter. Since 2017.

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press. Since 2006.

Member of the Editorial Board of Acta Informatica, published by Springer. Since 2015.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, published by Elsevier Science. Since 2000.

Member of the Editorial Board of LIPIcs: Leibniz International Proceedings in Informatics, Schloss Dagstuhl–Leibniz Center for Informatics. Since 2014.

Konstantinos Chatzikokolakis is:

Editorial board member of the 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, conferences and workshops.

8.1.4. Other Editorial Activities

Catuscia Palamidessi is/has been:

Co-editor (with Anca Muscholl and Anuj Dawar) of the special issue of Logical Methods in Computer Science dedicated to selected papers of ICALP 2017.

Co-editor (with Alexandra Silva and Natarajan Shankar) of the special issue of Logical Methods in Computer Science dedicated to selected papers of LICS 2015 and LICS 2016.

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 panel for the Research Evaluation for Development 2019 (RED19) of the Department of Computer Science and Engineering at the University of Gothenburg, Sweden.

Chair of the Nominating Committee for the 2019 renewal of the office holders of SIGLOG, the ACM Special Interest Group on Logic and Computation.

Member of the evaluation panel for the SU-ICT-03-2018: “Dynamic countering of cyber-attacks” - H2020 Work Programme 2018-2020.

Member of the evaluation panel for the program IKTPLUSS on Digital Security, Research Council of Norway (2018).

Member of the committee for the Alonzo Church Award for Outstanding Contributions to Logic and Computation. From 2015. In 2018 Palamidessi is the president of this committee.

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR (“Ministero dell’Istruzione, dell’Università e della Ricerca”). Since 2005.

President of the selection committee for the EATCS Best Paper Award. From 2006 until 2018.

Member of the EAPLS PhD Award Committee. From 2010.

8.1.6. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

CSL 2018. The 27th Computer Science Logic Annual Conference. Birmingham, UK, 4–7 September 2018.

CSF 2018. The 31st IEEE Computer Security Foundations Symposium, Oxford, UK, 9-12 July 2018.

PROOFS 2018 (Keynote speaker). The 7th International Workshop on Security Proofs for Embedded Systems. Amsterdam, The Netherlands, 13 September 2018.

PiMLAI 2018 Privacy in Machine Learning and Artificial Intelligence (FAIM 2018 Workshop). Stockholm, Sweden, 15 July 2018.

Bernoulli Symposium. Opening Symposium of the new institute for Artificial Intelligence, Mathematics, and Computer Science of the University of Groningen. Groningen, The Netherlands, 1 November 2018.

Konstantinos Chatzikokolakis has given invited talks at the following conference:

QEST 2018. 15th International Conference on Quantitative Evaluation of SysTems, Beijing, China, September 4-7, 2018.

8.1.7. Service

Catuscia Palamidessi has served as:

Member of the committee for the assignment of the Inria International Chairs. From 2017.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). From May 2016.

Konstantinos Chatzikokolakis has served as:

Member of the hiring committee for the "poste enseignants-chercheur Gaspard Monge", Ecole Polytechnique, 2018.

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, 2018.

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, 2018

Master : Konstantinos Chatzikokolakis has been teaching the masters course "Privacy Technologies", 40 hours, at the University of Athens, Greece. Oct - Dec, 2018.

8.2.2. Supervision

PhD in progress (2018-) Natasha Fernandez. Co-supervised Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Annabelle McIver. Thesis subject: Privacy Protection Methods for Textual Documents.

PhD in progress (2018-) Santiago Quintero. Co-supervised by Frank Valencia and Catuscia Palamidessi. Thesis Subject: Foundations of Group Polarization.

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 terminated (2016-18) Tymofii Prokopenko. Ecole Polytechnique and ENS Cachan. Grant Digiteo-Digicosme. Co-supervised by Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Serge Haddad (ENS Cachan). The PhD was terminated due to the lack of progress.

PhD in progress (2017-) Sergio Ramirez. Co-supervised by Frank Valencia and Camilo Rueda, Universidad Javeriana Cali. Thesis subject: Quantitive Spatial Constraint Systems.

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:

Vittoria Nardone (University of Sannio, Italy). PhD thesis reviewer. Title of the thesis: *Formal Methods for Android Applications*. Supervised by Antonella Santone. Defended in January 2019.

Antoine Dallon (ENS Paris-Saclay). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Verification of indistinguishability properties in cryptographic protocols - Small attacks and efficient decision with SAT-Equiv*. Supervised by Veronique Cortier and Stephanie Delaune. Defended on November 26, 2018.

David Mestel (University of Oxford). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Quantifying information flow*. Supervised by Bill Roscoe. Defended on October 26, 2018.

Jun Wang (University of Luxembourg). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Privacy-preserving recommender systems facilitated by machine learning approach*. Supervised by Qiang Tang and Peter Ryan. Defended on October 19, 2018.

Hamid Ebadi (Chalmers University, Sweden). Member of the committee board at the PhD defense. Title of the thesis: *Dynamic Enforcement of Differential Privacy*. Supervised by David Sands. Defended on March 5, 2018.

Catuscia Palamidessi has been examiner of the following habilitation thesis:

Elham Kashefi (LIP6, CNRS, France). Title of the thesis: *Verification of Quantum Computing*. Defended on February 8, 2018.

8.2.4. Other didactical duties

Catuscia Palamidessi has been:

Member of the advising committee for Hamid Ebadi, PhD student supervised by David Sands, Chalmers University, Sweden. From 2014 until 2018.

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. From 2014 until 2018.

8.3. Popularization

8.3.1. Education

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.

Catuscia Palamidessi has been:

- Invited speaker at PLMW@POPL 2019, the Programming Logic Mentoring Workshop 2019 (affiliated to POPL 2019). This workshop aims at encouraging graduate students and senior undergraduate students to pursue careers in programming language research, and at educating them on the research career.
- A participant in the round table at the FLOC Women in Logic workshop, a workshop organized to encourage women's presence in the logic community. Oxford, UK, 8 July 2018.

8.3.2. Interventions

Catuscia Palamidessi and Frank Valencia have supervised a group of high school children in stage d'observation. April 2018.

Catuscia Palamidessi has given an invited talk at:

- JNIM 2018. Journées Nationales 2018 du GDR Informatique Mathématique (Journée du 6 Avril en Hommage à Maurice Nivat). Palaiseau, France, 3-6 April 2018.

DATASPHERE Team

10. Dissemination

10.1. 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 promotes 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.

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Kavé Salamatian Organised the 3rd French-Japan CyberSecurity workshop in Annecy in April 2018.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Kavé Salamatian is professor at Université de Savoie.

Stéphane Grumbach is lecturer at SciPo Paris, where he teaches Master courses (M1, M2) on the Economy of Data. He also regularly gives lectures in universities, including ENA, ENS Lyon, Ecole centrale, Insa Lyon, etc.

10.2.2. Supervision

PhD in progress: Jingxiu Su, DNS data analysis, 2016, directeur de thèse Kave Salamatian

PhD in progress: Colin GERARD, Stratégies d'influence de la Russie sur les réseaux sociaux, 2018 PhD in progress with Institut Français de Géopolitique, sponsored by DGA, Director: Frederick Douzet

10.3. Popularization

Various publications have appeared in journals accessible to a larger audience [3], [2].

PESTO Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- J. Dreier: GRSRD 2018, Grande Region Security and Reliability Day 2018, Saarbrücken, March 2018 (co-chair with C. Rossow, CISPA, Germany)
- A. Imine: German-French PhD Workshop on Secure Big Data, October 24-26, 2018, Saarland, Germany (co-chair with S. Strohbach and Y. Zhang)

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- V. Cortier: POST 2018, E-VoteID 2018 (Track chair), CCS 2018, POST 2019, E-VoteID 2019 (Track chair), S&P 2019, CSF 2019
- A. Imine : DEXA 2018, SpaCCS 2018, TSP 2018, VLIoT@VLDB 2018, ICEIS 2019, DEXA 2019, VLIoT@VLDB 2019, C2SI 2019
- S. Kremer: Voting 2018, EuroS&P 2018, ESORICS 2018, EuroS&P 2019, Voting 2019, PERR 2019
- C. Ringeissen: IJCAR 2018, UNIF 2018, WRLA 2018, UNIF 2019, FroCoS 2019
- M. Rusinowitch: ICISSP 2018, IWSPA 2018, FPS 2018, CRISIS 2018

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- 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
- L. Vigneron: Technique et Sciences Informatiques, Lavoisier

10.1.4. Invited Talks

- V. Cortier. Keynote speaker of the 13th International Federated Conference on Distributed Computing Techniques (DisCoTec 2018), Madrid, Spain, June 2018.
- V. Cortier. Invited speaker at the Science and Society conferences, Nancy, May 15th, 2018.
- V. Cheval. Invited speaker at the African Conference on Research in Computer Science and Applied Mathematics (CARI 2018), Stellenbosch, South Africa, October 2018.

10.1.5. Scientific Expertise

ANR project expertise (A. Imine)

10.1.6. Research Administration

Inria evaluation committee (S. Kremer)

Inria Committee on Gender Equality and Equal Opportunities (S. Kremer, co-chair)

Jury Junior Research Position Inria Rennes-Bretagne Atlantique (S. Kremer)

Jury Senior Research Position Inria (S. Kremer)

Jury Professor at Univ Lorraine, LORIA (S. Kremer)

Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)

Scientific Council of the Computer Science CNRS Institute INS2I (V. Cortier)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence:

  J. Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 146 hours (ETD), TELECOM Nancy

  J. Dreier, Awareness for Cybersecurity, 7.5 hours (ETD), TELECOM Nancy

- Master:

  V. Cortier, Security of flows, 16 hours, M2 Computer Science, TELECOM Nancy and Mines Nancy

  J. Dreier, Introduction to Cryptography, 42 hours, M1 Computer Science, TELECOM 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, 32 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:

  J. Dreier, Symbolic verification of cryptographic protocols using Tamarin, 8 hours, 23rd Estonian Winter School in Computer Science (EWSCS), Palmse, Estonia

  V. Cheval. Verification of Security Protocols: From Confidentiality to Privacy, 4 hours, School organized within the 15th International Colloquium on Theoretical Aspects of Computing (ICTAC 2018), Stellenbosch, South Africa

  V. Cheval. Verification of Cryptographic Protocols, 2h30, 13th Summer School on Modelling and Verification of Parallel Processes (MOVEP 2018), Cachan, France

10.2.2. Supervision

- PhD defended in 2018:

  Antoine Dallon, Decision procedures for equivalence properties, November 26th, 2018 (V. Cortier and S. Delaune)

  Younes Abid, Automated Risk Analysis on Privacy in Social Networks, July 5th, 2018 (M. Rusinowitch)

  Alicia Filipiak, Conception and formal analysis of security protocols - one application to electronic voting and mobile paiement, March 23rd, 2018 (V. Cortier)

  Ludovic Robin, Vérification formelle de protocoles basés sur de courtes chaines authentifiées, February 15th, 2018 (S. Delaune and S. Kremer)

- PhD in progress:

  Ahmad Abboud, Compressed and Verifiable Filtering Rules in Software-defined Networking, started in August 2018 (A. Lahmadi, M. Rusinowitch and A. Bouhoula)

  Bizhan Alipour, Privacy protection against inference attacks in social networks, started in October 2018 (A. Imine, M. Rusinowitch)

  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)

10.2.3. Juries

Reviewer for Jonathan Hoyland PhD, Royal Holloway, UK (V. Cortier)

Reviewer for Jean-Karim Zinzindohoué PhD, ENS Paris (V. Cortier)

Reviewer for Nicolás Sebastián Gálvez Ramírez PhD, Univ Angers and UTFSM, Valparaíso (C. Ringeissen)

Reviewer for Vaishnavi Sundararajan PhD, Chennai (M. Rusinowitch)

10.3. Popularization

10.3.1. Articles and contents

(a voté) Euh non : a cliqué. V. Cortier, P. Gaudry, and S. Glondu. In Blog Binaire, Le Monde, March 2018 [42]

Interview for *Jeune Afrique* on electronic voting (V. Cortier).

Multiple interviews and articles on 5G security (*Est Républicain*, *CNRS Le Journal*, *The Conversation*, *Univers Freebox*, ...) (J. Dreier).

Interview for *News Tank RH* on electronic voting (S. Kremer).

Interview for *AFP* on electronic voting (S. Kremer).

Si c'est gratuit, C'est toi le produit. Université Participative de Vandoeuvre. *Est Républicain* (A. Imine).

Report on risks related to personal data disclosure. Equipe de L'Esprit Sorcier, February, (A. Imine).

10.3.2. Interventions

Presentation of security protocols to high school teachers in Computer Science, April 17th, 2018 (V. Cortier).

How to explain security protocols with Playmobil, Ada Lovelace Day, October 9th, 2018, (V. Cortier)

PRIVATICS Project-Team

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Antoine Boutet: Workshop on data transparency, 23/04/2018, Lyon, France.

Claude Castelluccia: APVP 2018, 3-6/06/2018, Porquerolles, France).

Claude Castelluccia: *Intelligence Oversight : Is Human Rights-Preserving Surveillance Possible?*, Grenoble Data institute, 25/01/2018, Grenoble, France.

8.1.1.2. Member of the Organizing Committees

Antoine Boutet: Winter School on Distributed Systems and Networks 2018, 4-8/02/2018, Sept Laux, France.

Antoine Boutet: SRDS 2018, 02-05/10/2018, Salvador, Brasil.

Mathieu Cunche: French GNURadio Days, 03/07/2018, INSA Lyon, France.

Daniel Le Metayer: Panel *Physical tracking: nowhere to hide*, CPDP 2018, 24/01/2018, Brussels, Belgium.

Vincent Roca: IEEE WiMob 2018.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

Antoine Boutet: Compas 2018, APVP 2018, Middleware 2018.

Mathieu Cunche: ACM WiSec 2018, Mobiquitous 2018, WCNC 2019, ICISSP 2018.

Claude Castelluccia: APF 2018.

Daniel Le Metayer: IWPE 2018, CPDP 2018, APF 2018.

Vincent Roca: SPACOMM 2018, SSCC 2018.

8.1.3. Invited Talks

Antoine Boutet: *Feedback on the Shonan Meeting on Anonymization methods and inference attacks*, 4th Franco-Japanese Cybersecurity workshop, 16/05/2018, Annecy, France.

Claude Castelluccia: *Cognitive security*, 4th Franco-Japanese Cybersecurity workshop, 16/05/2018, Annecy, France.

Claude Castelluccia: *Brain Hacking*, College des Bernardins, 11/12/2018, Paris, France.

Claude Castelluccia: *Plateforme en ligne et transparence*, AFDIT, 09/11/2018, Paris, France.

Claude Castelluccia: *Internet Surveillance*, Intelligence Oversight workshop, 25/01/2018, Grenoble, France.

Cédric Lauradoux: *Cybersécurité et cybermenaces*, Club Democraties, 09/03/2018, Paris, France.

Cédric Lauradoux: *Cybersécurité et cybermenaces*, Rectorat Académie de Grenoble, 10/12/2018, Grenoble, France.

Daniel Le Metayer, *Intelligility and transparency in machine learning and AI*, Société Française de Statistique, 18/05/2018, Paris, France.

Daniel Le Metayer, *Transparency and opacity in IT systems*, INSA Lyon CITI, 23/04/2018, Lyon, France.

Vincent Roca, *Privacy and Connected Objects*, Eclipse IoT Days Grenoble, 18/01/2018, Grenoble, France.

Vincent Roca, *Archéologie de la fuite de nos données personnelles par le biais de nos téléphones*, Atelier Internet – ENSIIB, 06/04/2018, Lyon, France.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Antoine Boutet, *Privacy*, 12h, INSA-Lyon, France.

Master : Antoine Boutet, *Security*, 12h, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, *Introduction to computer science*, 120h, L1, INSA-Lyon, France.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.

Undergraduate course : Mathieu Cunche, *Security & Privacy*, 21h, L3, INSA-Lyon, France.

Master : Mathieu Cunche, *Privacy and Data protection*, 14h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, *Cryptography and Communication Security*, 18h, M1, INSA-Lyon, France.

Master : Cédric Lauradoux, *Advanced Topics in Security*, 20h, M2, Ensimag/INPG, France.

Master : Cédric Lauradoux, *Systems and Network Security*, 30h, M1, Ensimag, France.

Master : Cédric Lauradoux, *Internet Security*, 12h, M2, University of Grenoble Alpes, France.

Master : Cédric Lauradoux, *Cyber Security*, 3h, M2, Laws School of University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.

Master : Claude Castelluccia, *Cyber Security*, 6h, M2, Laws School of University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Data Privacy*, 6h, M2, Laws School of University of Grenoble Alpes, France.

Master : Daniel Le Metayer, *Privacy*, 12h, M2 MASH, Université Paris Dauphine, France.

Master : Daniel Le Metayer, *Privacy*, 12h, M2, Insa Lyon, France.

Master : Vincent Roca, *On Wireless Communications*, 12h, M1, Polytech' Grenoble, France.

Undergraduate course : Vincent Roca, *On Network Communications*, 44h, L1, IUT-2 (University of Grenoble Alpes), France.

Undergraduate course : Vincent Roca, *On Security and Privacy in smartphones*, 6h, L-Pro, University of Grenoble Alpes, France.

Master : Vincent Roca, *On Security and Privacy in smartphones*, 3h, M2, France.

8.2.2. E-learning

E-learning

Mooc: Cédric Lauradoux and Vincent Roca, *, 2 month session, FUN-MOOC, Inria, public ciblé, 23000 (13000 first session and 10000 second session).*

8.2.3. Supervision

- 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 Le Métayer.
- PhD in progress : Supryia Adhatarao, *Privacy of E-learning systems* , March 2018, Cédric Lauradoux.
- PhD in progress : Coline Boniface, *Cyberweapons: from bug bounties to zero days* , March 2018, Cédric Lauradoux.
- PhD in progress : Raoul Kerkouche, *Privacy-Preserving Processing of Medical Data* , January 2018, Claude Castelluccia.
- PhD in progress : Clement Henin, *Explainable AI* , September 2018, Claude Castelluccia et Daniel Le Metayer.
- PhD in progress: Théo Jourdan, *Privacy-preserving machine learning in medical domain, October 2018, Antoine Boutet.*
- *Intern (M2): Louis Beziaud,* Privacy of national identity systems*, M2 ENS Rennes, Claude Castelluccia et Daniel Le Metayer.*
- *Intern (L3): Alexandre van Beurden, Inspect what location history reveals about an individual, Antoine Boutet.*
- *Intern (L3): Romain Fournier, Development of a cybersecurity platform, Antoine Boutet.*
- *Intern (L3): Bastien Durand, Analysis of the correlation between the mobility and the personality of an individual, Antoine Boutet.*

8.2.4. Juries

PhD: David Gerault, *Security Analysis of Contactless Communication Protocols*, Université Clermont Auvergne , 27/11/2018, Cédric Lauradoux.

PhD: Jonathan Detchart, *Optimisation de codes correcteurs d'effacements par application de transformées polynomiales*, Université de Toulouse, 05/12/2018, Vincent Roca.

PhD: Elise Tourne, *Le phénome de circulation des données à caractère personnel dans le cloud: étude de droit matériel dans le contexte de l'Union Européenne*, Université Lyon 3, 11/06/2018, Daniel Le Métayer.

8.3. Popularization

8.3.1. Hearings

- Claude Castelluccia: *Understanding Algorithmic Decision-Making Systems*, European Parliament, 10/2018, Strasbourg, France.
- Daniel Le Metayer: *Understanding Algorithmic Decision-Making Systems*, European Parliament, 10/2018, Strasbourg, France.
- Daniel Le Metayer: *Transparence et explicabilité des algorithmes d'aide à la décision*, CCNE, 02/2018, Paris, France.

8.3.2. Internal or external Inria responsibilities

- Claude Castelluccia is co-leader of the Worpackage 5 (data governance and privacy) of the Grenoble Data Institute.
- Claude Castelluccia is co-leader of Grenoble CyberAlps (cybersecurity institute of Grenoble).
- Daniel Le Metayer chairs the CNIL-Inria privacy award.
- Vincent Roca is co-editor of the white book *Cybersecurity: current challenges and Inria's research directions*.

8.3.3. Articles and contents

- Claude Castelluccia: *Manipulation informationnelle et psychologique*, Le blog binaire du Monde, 05/2018.
- Claude Castelluccia: *Data surveillance and manipulation*,Interview for Magazine Capital, 12/2018.
- Mathieu Cunche: *Cybersécurité et menace informatique*, Sommet des start-up sciencesetavenir.fr, 11/2018, Lyon, France.
- Mathieu Cunche: *Attaque par déni de service dans le Wi-Fi*, GNULinux Magazine HS 99, 11/2018.
- Mathieu Cunche: *Comprendre les attaques Krack*, GNULinux Magazine HS 99, 11/2018.
- Daniel Le Metayer: *Weighting the impact of the GDPR*, Communications of the ACM, 11/2018.
- Daniel Le Metayer: *Qui gouverne les algorithmes ?*, Revue THIIRD, 11/2018.
- Vincent Roca: Inria White Paper in Cyber-Security.

8.3.4. Education

- Cédric Lauradoux: *Action nombres et cryptographie*, Maison pour la science, Inria, 06/02/2018, Grenoble, France.
- Cédric Lauradoux: *Action nombres et cryptographie*, Maison pour la science, 18/12/2018, Annecy, France.
- Cédric Lauradoux: *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, 02-03/2018.
- Cédric Lauradoux: : *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, 11-12/2018.

8.3.5. Interventions

- Cédric Lauradoux: *Atelier cryptograpie*, Fête de la Science, 11-12/10/2018, Grenoble, France.
- Cédric Lauradoux: *Cryptologie et Vie privée*, Semaine des mathématiques, Lycée Gabriel-Faure, 15/03/2018, Tournon, France.
- Cédric Lauradoux: *Cryptologie et Vie privée*, Semaine des mathématiques, Lycée Boissy d'Anglas, 16/03/2018, Annonay, France.
- Cédric Lauradoux: *Challenge de cryptologie*, MathC2+ internship, 26/06/18, Grenoble, France.
- Cédric Lauradoux: *Challenge de cryptologie*, Cité scolaire Jean PREVOST, 02/06/2018, Villard de Lans, France.
- Cédric Lauradoux: *Challenge de cryptologie*, Collège Barnave, 18/01/2018, Saint-Égrève, France.

8.3.6. Internal action

- Cédric Lauradoux: *Réglementation sur les données*, Inria, Grenoble, 19/06/2018.
- Cédric Lauradoux: *Réglementation sur les données*, IMAG, Grenoble, 09/07/2018.

PROSECCO Project-Team

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. General Chair, Scientific Chair

- Catalin Hritcu and Amal Ahmed co-organized a Dagstuhl Seminar on Secure Compilation (18201)
- Harry Halpin and Bart Preneel co-organized the ECRYPT-CSA workshop on Crypto Policies (22-23 January 2018) in Brussels, Belgium.

9.1.1.2. Member of the Organizing Committees

- Catalin Hritcu and Amal Ahmed were organizers for PriSC 2018 and the upcoming PriSC 2019

9.1.2. Scientific Events Selection

9.1.2.1. Chair of Conference Program Committees

- Catalin Hritcu was the PC chair for the 2nd Workshop on Principles of Secure Compilation (PriSC) at POPL 2018
- Harry Halpin was General Chair of the 1st Workshop on the Decentralization of Governance at INSCI 2018

9.1.2.2. Member of the Conference Program Committees

- Bruno Blanchet was PC member of RESSI 2018 (*Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*).
- Catalin Hritcu was PC member of EuroS&P 2018, ESOP 2018, and CCS 2018
- Karthikeyan Bhargavan was PC member of IEEE S&P 2018, ACM CCS 2018, and POST 2018
- Harry Halpin was PC Member of SSR 2018, ACM WWW 2018, and ISWC 2018.

9.1.2.3. Reviewer

- Catalin Hritcu served as a reviewer for the Journal of Automated Reasoning (JAR)

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

- Catalin Hritcu gave an Invited Keynote talk at the Working Formal Methods Symposium (FROM) in June 2018
- Catalin Hritcu gave invited talks at Nomadic Labs (Tezos), IRIF Verification Seminar (Paris 7), and SoSySec seminar (IRISA Rennes)
- Karthikeyan Bhargavan gave invited talks at Security Standardization Research (SSR 2018), Formal Methods and Tools for Security (FMATS 2018), Crypto Welcomes TLS 1.3 (CWTLS), and the annual GDR Securité meeting.
- Harry Halpin gave invited talks at the EPFL Summer Research Institute in July 2018, the Web 3.0 Summit in October 2018, and Binance Labs in December 2018.

9.1.5. Leadership within the Scientific Community

- Catalin Hritcu served as the Artifact Evaluation Co-Chair for POPL 2018 and POPL 2019

9.1.6. 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.
- Bruno Blanchet participated to a review of the code of the Tezos blockchain by the Inria Foundation (March–May 2018).
- Harry Halpin participated as a member of the advisory board to the PANORAMIX EC H2020 project (2018).

9.1.7. Research Administration

- Bruno Blanchet was co-president of the Inria hiring committee for PhD, post-docs, and *délégations* (*Commision des Emplois Scientifiques*, CES).
- Bruno Blanchet was representative of Inria Paris at the DIM RFSI (*Domaine d'Intérêt Majeur, Réseau Francilien en Sciences Informatiques*).

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Master: Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII, France
- Master: Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII, France
- Master: Karthikeyan Bhargavan, Network Protocol Safety and Security, 18h equivalent TD, ACN master, Telecom ParisTech
- PhD: Formally Secure Compartmentalizing Compilation course at International School on Foundations of Security Analysis and Design (FOSAD), 27-28 August, 2018, Bertinoro, Italy
- PhD: Program Verification with F* course at EPIT 2018 Software Verification Spring School, 7-11 May, 2018, Aussois, France
- PhD: Attacks and Automated Tools, BIU winter school on cryptography, 11-15 February, 2018, Tel Aviv, Israel
- PhD: Crypto standards for the Internet and Web. ECRYPT-CSA School on Societal Aspects of Cryptology and on Business and Innovation in Crypto. 7-9 January. Zurich, Switzerland.
- PhD: Mix networking, ECRYPT Summer School, ECRYPT-NET School on Integrating Advanced Cryptography with Applications, 16-21 September 2018, Kos, Greece.

9.2.2. Supervision

- PhD: Jean Karim Zinzindohoue, Secure, Fast and Verified Cryptographic Applications: A Scalable Approach [13], ENS Paris, defended on July 3, 2018, supervised by Karthikeyan Bhargavan.
- PhD: Nadim Kobeissi, Formal Verification for Real-World Cryptographic Protocols and Implementations [12], ENS Paris, defended on December 10, 2018, supervised by Karthikeyan Bhargavan and Bruno Blanchet.
- PhD in progress: Benjamin Beurdouche, on verified cryptographic protocol implementations, ENS Paris, since October 2016, supervised by Karthikeyan Bhargavan.
- PhD in progress: Marina Polubelova, on verified post-quantum cryptography, PSL Paris, since October 2017, supervised by Karthikeyan Bhargavan.

- PhD in progress: Natalia Kulatova, on verified secure hardware APIs, PSL Paris, since October 2017, supervised by Karthikeyan Bhargavan.
- PhD in progress: Denis Merigoux, on verified RUST applications, PSL Paris, since November 2017, supervised by Karthikeyan Bhargavan.
- PhD in progress: Benjamin Lipp, On Mechanised Cryptographic Proofs of Protocols and their Link with Verified Implementations, ENS Paris, since October 2018, supervised by Bruno Blanchet and Karthikeyan Bhargavan.
- PhD in progress: Kenji Maillard, on Semantic Foundations for F*, started January 2017, supervised by Catalin Hritcu and Karthikeyan Bhargavan
- PhD in progress: Carmine Abate, The Formal Foundations of Secure Compilation, since June 2018, advised by Catalin Hritcu and Bruno Blanchet
- PhD in progress: Jérémy Thibault, Secure Compartmentalizing Compilation to a Tagged Architecture, from August 2018, advised by Catalin Hritcu and Bruno Blanchet
- PhD in progress: Guido Martínez (CIFASIS-CONICET Rosario), Metatheory for Semi-Automatic Verification of Effectful Programs, from April 2017, advised by Mauro Jaskelioff (CIFASIS-CONICET Rosario) and Catalin Hritcu

9.2.3. Juries

- Karthikeyan Bhargavan participated in the PhD jury of Daniel Fett at University of Stuttgart.
- Harry Halpin participated in the PhD jury of Joseph Raad at University Paris-Saclay.

9.3. Popularization

9.3.1. Internal or external Inria responsibilities

- Bruno Blanchet was co-president of the Inria hiring committee for PhD, post-docs, and *délégations* (*Commision des Emplois Scientifiques*, CES).
- Bruno Blanchet was representative of Inria Paris at the DIM RFSI (*Domaine d'Intérêt Majeur, Réseau Francilien en Sciences Informatiques*).

9.3.2. Interventions

- Karthikeyan Bhargavan was a panelist at the Cloudflare Internet Summit in London, June 14, 2018.
- Harry Halpin was a panelist at the World Digital Asset Summit in San Fransisco, USA, December 10, 2018.

TAMIS Project-Team

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Selection

10.1.1.1. Member of Conference Steering Committees

- Olivier Zendra is a founder and a member of the Steering Committee of ICOOOLPS (International Workshop on Implementation, Compilation, Optimization of OO Languages, Programs and Systems)

10.1.1.2. Chair of Conference Program Committees

- Olivier Zendra was co-chair of the Program Committee and the Organizing Committee of the 13th Workshop on Implementation, Compilation, Optimization of Object-Oriented Languages, Programs and Systems (ICOOOLPS 2018)

10.1.1.3. Member of the Conference Program Committees

- Stefano Sebastio was a PC member of IEEE SOCA 2018 and ICORES 2019
- Annelie Heuser was PC member of TCHES 2018, CARDIS 2018, PROOFS 2018, KANGACRYPT 2018.

10.1.1.4. Reviewer

- Stefano Sebastio was a reviewer for ICORES 2019, IEEE SOCA 2018, CRiSIS 2018, COORDINATION 2018, MeTRiD satellite workshop of ETAPS 2018

10.1.2. Journal

10.1.2.1. Reviewer - Reviewing Activities

- Stefano Sebastio was a reviewer for EJOR (European Journal of Operational Research), OptimLett (Optimization Letters), JCST (Journal of Computer Science and Technology), IJCC (International Journal of Cloud Computing), IJDSN (International Journal of Distributed Sensor Networks)

10.1.3. Scientific Expertise

- Olivier Zendra is a CIR expert for the MENESR.
- Olivier Zendra participated to the CRHC and CRCN national juries for Inria as a member of Inria’s evaluation committee.
- Olivier Zendra participated to a MCF recruiting committee for IUT de Vannes.
- Olivier Zendra is a member of the editorial board and co-author of the “HiPEAC 2019 Vision”
- Olivier Zendra is a member of Inria’s evaluation committee.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Eduard Baranov: Master Méthodes d’analyse de risques, M2, Université de Bretagne Sud, France
- Tania Richmond: ENS Ker Lan.

10.2.2. Supervision

- PhD in progress: Christophe Genevey Metat (Rennes 1): , October 2018, Jean-Marc Jezequel, Benoit Gerard, Annelie Heuser and Clementine Maurice

- PhD in progress : Olivier Descourbe, On Code Obfuscation, October 2016, Axel Legay and Fabrizio Biondi.
- PhD in progress : Alexandre Gonsalvez, On Obfuscation via crypto primitives, April 2016, Axel Legay and Caroline Fontaine.
- PhD in progress : Nisrine Jafri (Rennes1), On fault Injection detection with MC of Binary code, December 2015, Axel Legay and Jean-Louis Lanet.
- PhD in progress : 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

- Annelie Heuser was a referee for the PhD defense of Eleonora Cagli (CEA - Commissariat à l'Energie atomique et aux Energies alternatives, Grenoble)
- Annelie Heuser was a referee for the PhD defense of Damien Marion (Telecom ParisTech, CIFRE with Secure-IC)