Activity Report 2019

# Section Dissemination

SECURITY AND CONFIDENTIALITY

<h1 style="color:red; text-align:center">ARIC Project-Team</h1>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

- Damien Stehlé organized a Winter School on the mathematical foundations of public-key cryptography, in Aussois (France), from March 17 to March 22.
- Bruno Salvy was a co-chair of AofA'2019 (Analysis of Algorithms), in Luminy, France.

### 10.1.2. Scientific Events: Selection

- Elena Kirshanova was in the program committee of Asiacrypt 2019.
- Benoît Libert was in the program committees of PKC 2019 and PKC 2020.
- Nathalie Revol is in the steering committee of the Arith conference series. She was in the program committee of Arith'26, of Correctness 2019 (workshop of SuperComputing) and of PPAM (Parallel Processing and Applied Mathematics) 2019.
- Bruno Salvy is in the steering committee of AofA. He was in the program committee for FPSAC 2019 and in the scientific committee of OPSFA 2019. He is in the program committee for AofA 2020.
- Damien Stehlé is in the steering committee of the PQCrypto conference series. He was in the program committee PQCrypto 2019 and is in the program committee of PQCrypto 2020. He was in the program committee of CRYPTO 2019.
- Gilles Villard was in the program committee of ISSAC 2019.

### 10.1.3. Journal

- Benoît Libert was a member of the editorial board of IET Information Security until July 31, 2019.
- Jean-Michel Muller is associate editor in chief of the IEEE Transactions on Emerging Topics in Computing.
- Nathalie Revol is a member of the editorial board of Reliable Computing.
- 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 of the journal *Annals of Combinatorics*.
- Damien Stehlé is a member of the editorial board of Journal of Cryptology.

### 10.1.4. Invited Talks

- Claude-Pierre Jannerod gave an invited talk at the workshop *Structured Matrix Days* (Limoges, May 23–24, 2019).
- Benoît Libert gave an invited presentation during the "Workshop on Modern Trends in Cryptography" organized at Nanyang Technological University (Singapore) on June 13-14, 2019.
- Damien Stehlé gave lectures during the "Euclidean lattices: theory and applications" Summer school that was held in Kaliningrad (Russia), from July 15 to July 19.

### 10.1.5. Leadership within the Scientific Community

- Guillaume Hanrot was a member of selection committees for professors at Université de Lorraine (in CS) and at Université de Nouvelle-Calédonie (in Mathematics). He was also in the hiring committee of the computer science department of École polytechnique. He is a member of the working group on the revision of the CS curriculum in *Classes préparatoires aux grandes écoles*.

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

- Jean-Michel Muller is co-head of the GDR Informatique Mathématique of the CNRS. He is also a member of the Scientific Council of CERFACS (Toulouse).

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

- Nathalie Revol is a member of the steering committee of GDR Calcul; she was a member of the hiring committee (Comité de Sélection) for 2 positions at U. Nantes.

- Bruno Salvy is a member of the scientific councils of the CIRM, Luminy and of the GDR Informatique Mathématique of the CNRS.

### 10.1.6. Scientific Expertise

- Nathalie Revol has been an expert for the European H2020 program.

### 10.1.7. Research Administration

- Jean-Michel Muller is a member of the *Commission Administrative Paritaire* (CAP) *Directeurs de Recherches* of CNRS.

- 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: Guillaume Hanrot, Computer algebra, 10h, ENS de Lyon, France
- Master: Guillaume Hanrot, Cryptanalysis, 15h, ENS de Lyon, France
- Master: Claude-Pierre Jeannerod, Computer Algebra, 18h, M2Pro ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1, France
- Master (1&2): Fabien Laguillaumie, Cryptography, 160 h, ISFA, UCBL, France
- Master: Benoît Libert, Advanced Topics in Cryptography, 15h, ENS de Lyon, France
- Master: Nicolas Louvet, Compilers, 22h, M1, UCB Lyon 1, France
- Master: Alain Passelègue, Computer Algebra, 10h, M1, ENS de Lyon, France
- Master: Alain Passelègue, Advanced Topics in Cryptography, 30h, M2, ENS de Lyon, France
- Master: Nathalie Revol, Numerical Algorithms and Reliability, 12h, M2Pro ISFA (Institut de Science Financière et d'Assurances), Université Claude Bernard Lyon 1, France
- Master: Bruno Salvy, Computer Algebra, 6h, ENS de Lyon, France
- Master: Bruno Salvy, Logic and Complexity, 32h, École polytechnique, France
- Master: Damien Stehlé, Cryptanalysis, 15h, ENS de Lyon, France
- Master : Gilles Villard, Computer Algebra, 8h, ENS de Lyon, France
- Bachelor: Guillaume Hanrot, Calculability and complexity, 32h, ENS de Lyon, France
- Bachelor: Nicolas Louvet, Computer Architecture, 27h, L1, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Operating Systems, 50h, L2, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 24h, L2, UCB Lyon 1, France

- Bachelor: Nicolas Louvet, Data Structures and Algorithms, 40h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Formal Languages, 15h, L3, UCB Lyon 1, France
- Bachelor: Nicolas Louvet, Classical Logic, 15h, L3, UCB Lyon 1, France
- Bachelor: Bruno Salvy, Design and Analysis of Algorithms, 20h, École polytechnique, France

### 10.2.2. Supervision

- PhD: Florent Bréhard, Certified Numerics in Function Spaces: Polynomial Approximations Meet Computer Algebra and Formal Proof, ENS de Lyon, July 12, Nicolas Brisebarre (co-supervision with Mioara Joldes, CNRS LAAS, and Damien Pous, LIP)
- PhD: Alice Pellet-Mary, On ideal lattices and the GGH13 multilinear map, ENS de Lyon, October 16, Damien Stehlé
- PhD: Chen Qian, Lossy Trapdoor Primitives, Zero-Knowledge Proofs and Applications, IRISA Rennes, October 4, Benoît Libert (co-supervision with Pierre-Alain Fouque, IRISA)
- PhD in progress: Miruna Rosca, The middle-product learning with errors problem, January 2017, Damien Stehlé
- PhD in progress: Huyen Nguyen, Cryptographic aspects of orthogonal lattices, September 2018, Damien Stehlé
- PhD in progress: Radu Titiu, Advanced cryptographic primitives based on standard assumptions, January 2017, Benoît Libert
- PhD in progress: Adel Hamdi, Functional Encryption, December 2017, Fabien Laguillaumie (co-supervised by Sébastien Canard, Orange)
- PhD in progress: Ida Tucker, Advanced cryptographic primitives from homomorphic encryption, October 2017, Fabien Laguillaumie (co-direction with Guilhem Castagnos, Université de Bordeaux)

### 10.2.3. Juries

- Damien Stehlé was a jury member for the PhD defences of Ilia Iliashenko (K.U. Leuven, Belgium) and Joost Rijneveld (Radboud U., the Netherlands) and for the habilitation defence of Omar Fawzi (ENS de Lyon). He was a reviewer and jury member of the PhD of Thomas Debris-Alazard (Sorbonne U.) and for the habilitation of Guilhem Castagnos (U. Bordeaux).
- Benoît Libert was a reviewer for the PhD theses of Romain Gay (ENS Paris), Jérémy Chotard (Univ. of Limoges). He was a PhD examiner for the thesis of Andrea Cerulli (University College London, United Kingdom). He also chaired the PhD committee of Anca Nitulescu (ENS Paris).
- Fabien Laguillaumie was reviewer and jury member of the PhD of Pauline Bert (Université de Rennes) and of the HDR of Olivier Blazy (Université de Limoges)
- Jean-Michel Muller was reviewer and jury member of the PhD of Clothilde Jeangoudoux (Sorbonne University, Paris)
- Gilles Villard was reviewer for the PhD thesis of Robin Larrieu (Université Paris-Saclay); examiner for the habilitation of Pascal Giorgi (Université de Montpellier) and the PhD thesis of Matías Bender (Sorbonne Université).

## 10.3. Popularization

### 10.3.1. Internal or external Inria responsibilities

- Nathalie Revol was in the scientific committee for the Journées Scientifiques Inria (Lyon, 5-7 June 2019).
- Nathalie Revol was a member of the editorial committee of interstices; she is the scientific editor of this Web magazine since September 2019.
- Nathalie Revol belonged to the steering committee of MMI (Maison des Mathématiques et de l'Informatique) until July 2019; she is now a member of its prospective committee.
- 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, launched in February 2019.

### *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.
- Nathalie Revol works with DANE (Délégation Académique au Numérique dans l'Éducation) of Rectorat de Lyon towards educating primary school teachers, by educating educators (e-RUN); she is a member of the Conseil Scientifique du Numérique.
- Nathalie Revol presented activities for teaching computer science at every school level, and in particular activities led by Inria, for a Taiwanese delegation (Grenoble, October 2019).

### *10.3.4. Interventions*

- Nathalie Revol spent 2 days at école Guilloux, with 50 pupils aged 10 (level: CM2), to teach computer science without any computer (so-called "unplugged computer science"): data, algorithms, networks.
- For high-school pupils ($\simeq 150$ pupils): as an incentive, especially for girls, to choose scientific careers, Nathalie Revol gave talks at Mondial des Métiers (in February 2019), collège Jean Zay (Brignais, March 2019) and Girls Can Code (Lyon, August 2019). With Jérôme Germoni and Natacha Portier, she organized a day *Filles & Info* in November 2019, gathering about 70 high-school girls of 1e and Terminale.
- For a larger audience: she took part to Pop Science, doing magic tricks in the street at La Duchère, Lyon, May 2019; with Florent Masséglia, she introduced 5 important figures of computer science, chosen among the personalities of the "7 families of computer science" playcard, for L'Esprit Sorcier, for la Fête de la Science, Paris, October 2019, cf https://www.youtube.com/watch?v=ypnQe91Pztc
- Nathalie Revol took part to a day of teaching unplugged computer science for whoever was interested, at La Gaîté Lyrique, Paris, June 2019.

### *10.3.5. Creation of media or tools for science outreach*

Nathalie Revol belongs to the working group "Informatique Sans Ordinateur", which creates unplugged activities to teach computer science; this group meets twice a year, usually in Lyon.

# AROMATH Project-Team

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Organisation

#### 8.1.1.1. General Chair, Scientific Chair

Laurent Busé organized a CIMPA school at Joao Pessoa, Brazil, November 4-13, on the topic "Syzygies: from theory to applications". Six courses delivered by international experts of this topic were scheduled during this school that hosted about 40 international PhD students and young researchers. For more details, see http://www-sop.inria.fr/members/Laurent.Buse/CimpaSchoolBrazil/.

#### 8.1.1.2. Member of the Organizing Committees

Laurent Busé co-organized with C. D'Andrea and Y. Cid Ruiz a mini-symposium on «Syzygies and Applications to Geometry » at the SIAM Conference on Applied Algebraic Geometry, Bern, Switzerland, July 9-13, 2019.

Angelos Mantzaflaris and Bernard Mourrain co-organized with E. Tsigaridas a mini-symposium on "Symbolic-numeric methods for non-linear equations: Algorithms and applications" at the SIAM Conference on Applied Algebraic Geometry, Bern, Switzerland, July 9-13, 2019.

### 8.1.2. Scientific Events: Selection

#### 8.1.2.1. Member of the Conference Program Committees

Laurent Busé was a member of the international program committee of the 2019 Symposium on Physical and Solid Modeling (SPM), Vancouver, Canada, June 17-19. He was also a member of the scientific committee fro the conference "Ideals, Varieties, Applications" celebrating the influence of David Cox, Amherst, USA, June 10-14.

Angelos Mantzaflaris served in the PC of the 2019 Solid and Physical Modeling (SPM), https://project.inria.fr/spm2019/.

#### 8.1.2.2. Reviewer

Laurent Busé reviewed for *Symposium on Physical and Solid Modeling conference*, *SIGGRAPH conference*, *ISSAC conference* and *MEGA conference*.

Ioannis Emiris reviewed for the *Symposium of Computational Geometry*, *ICALP: Intern. Conf. Automata, Logic & Programming* and *MEGA: Méthodes Effectives en Géométrie Algébrique*.

Angelos Mantzaflaris reviewed for the  *Symposium on Physical and Solid Modeling*.

Bernard Mourrain reviewed for *Symposium on Physical and Solid Modeling conference*, *ISSAC conference* and *MEGA conference*.

### 8.1.3. Journal

#### 8.1.3.1. Member of the Editorial Boards

Ioannis Emiris is editorial board member of *J. Symbolic Computation (Elsevier)* and *Mathematics for Computer Science (Springer)*.

Evelyne Hubert is on the editorial board of Foundation of Computational Mathematics (since 2017) and the Journal of Symbolic Computation (since 2007).

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).

*8.1.3.2. Reviewer - Reviewing Activities*

Laurent Busé reviewed for *Graphical Models journal*, *Advances in Applied Mathematics journal*, *SIAM SIAGA journal*, *International Mathematics Research Notices*, *Journal of Algebra*, *Applicable Algebra in Engineering, Communication and Computing journal*, *Computer-Aided Design journal*, *Computer Aided Geometric Design journal*, *Journal of Computer Science and Technology*, *AMS Mathematics of Computations journal*, *Israel Journal of Mathematics* and *Journal of Symbolic Computation*.

Evelyne Hubert reviewed for Journal für die reine und angewandte Mathematik, Proceedings of the American Mathematical Society, Advances in Applied Mathematics, Foundation of Computational Mathematics, SIAM Journal on Applied Algebra and Geometry, Journal of Symbolic Computation, and Computer Aided Geometric Design.

Bernard Mourrain reviewed for *Annales Henri Lebesgue*, *Collectanea Mathematica journalComputer-Aided Design journal*, *Computer Aided Geometric Design journal*, *Journal of Global Optimization*, *Journal of Symbolic Computation*, and *Mathematics of Computations journal*,

Angelos Mantzaflaris reviewed for Computer Methods in Applied Mechanics and Engineering, Computer Aided Geometric Design, Computers & Mathematics with Applications, and Journal of Symbolic Computation.

### 8.1.4. Invited Talks

Ahmed Blidia was an invited speaker in the minisymposium *Multivariate spline approximation and algebraic geometry* at SIAM Applied Algebraic Geometry meeting, Bern, Switzerland in June 2019.

Laurent Busé was invited to give two lectures at the "27th National School on Algebra: Graded modules over polynomial rings with applications to free divisors", Bucarest, Romania, May 19-25; he was invited to give a plenary talk at the conference "Ideals, Varieties, Applications", in honor of David Cox, Amherst, USA, June 10-14; he gave an invited course during the school "TIME2019: Curves and Surfaces, a History of Shapes", Levico Terme, Italy, Septembre 2-6.

Ioannis Emiris was an invited speaker at KAUST, Visual computing center, Saudi Arabia in February 2019, and SIAM Applied Algebraic Geometry meeting, Bern, Switzerland in June 2019.

Alvaro Fuentes Suarez gave a seminar talk in the MFX team at Inria NGE in February 2019.

Evelyne Hubert presented a series of lectures at the national conference *Equations Fonctionnelles et Interactions* (Anglet). She was invited to give talks at the $A^3$ - *Arctic Applied Algebra* conference (Tromsø, Norway, April 2019) and the conference *A celebration of Symmetry and Comptutation* (Canterburry, UK). She delivered seminar talks at the University of the Arctic (Tromsø, Norway) and at the Isaac Newton Institute (Cambridge, UK).

Angelos Mantzaflaris gave an invited talk at the 4th Workshop of the ERC project CHANGE, Centro Congressi dell'Annunziata, Sestri Levante, Italy (November 2019) and at the Schloss Dagstuhl – Leibniz Center for Informatics seminar on Interactive Design and Simulation, Germany (December 2019). He also delivered a mini-symposium presentation at the annual conference on Isogeometric Analysis (IGA 2019, Munich, Germany, September 2019).

Both Angelos Mantzaflaris and Bernard Mourrain were invited at the meeting on "Isogeometric Splines: Theory and Applications" of the Banff International Research Station for Mathematical Innovation and Discovery (BIRS, February 2019), at the Oberwolfach Mini-Workshop on Mathematical Foundations of Isogeometric Analysis (July 2019), and at the Algebraic Spline Geometry Meeting in Swansea, UK (August 2019).

Bernard Mourrain was invited to give a talk at the conference $A^3$ - *Arctic Applied Algebra* (Tromsø, Norway, April 1-4); an invited speaker of the conference MEGA (Madrid, Spain, June), to talk at the minisymposium *The algebra and geometry of tensors* of SIAM Applied Algebraic Geometry meeting, (Bern, Switzerland, June 2019), at the conference *Multivariate Approximation and Interpolation with Applications* (Vienna, Austria, Aug. 26-30), at the Italian Mathematical Union conference (Pavia, Sept. 2-5).

He was also invited to give two courses on splines at the University of Montpellier, (October 23-24, 2019).

Erick Rodriguez Bazan was an invited speaker in the minisymposium *Symmetry in algorithmic questions of real algebraic geometry* at SIAM Applied Algebraic Geometry meeting, Bern, Switzerland in June 2019.

Fatmanur Yildirim was an invited speaker in the minisymposium *Syzygies and applications to geometry* at SIAM Applied Algebraic Geometry meeting, Bern, Switzerland in June 2019.

### 8.1.5. Leadership within the Scientific Community

Ioannis Emiris is member of the Scientific Board of Hellenic Foundation for Research & Innovation (http://www.elidek.gr), representing Informatics and Mathematics.

Bernard Mourain has been elected vice chair of the SIAM Algebraic Geometry group.

### 8.1.6. Scientific Expertise

Evelyne Hubert was on the hiring committee for Junior Research Scientists at Inria NGE.

### 8.1.7. Research Administration

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

Evelyne Hubert was a member of Inria Evaluation committee (until June 2019).

Laurent Busé is a member of the admnistrative and scientific committee of the labex AMIES. He is also member of the CDT at Inria Sophia-Antipolis and the CPRH of the Mathematics Laboratory Jean-Alexandre Dieudonné of the University of Nice.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

- Licence : Ioannis Emiris, Discrete Math, 52 h (L1), NKU Athens
- Licence : Ioannis Emiris, Software development, 26 h (L3), NKU Athens
- Master : Ioannis Emiris, Geometric data science, 52 h (M2), NKU Athens
- Master : Ioannis Emiris, Structural bioinformatics, 39 h (M2), NKU Athens
- Master : Laurent Busé, Geometric Modeling, 18h (M2), engineer school of the University of Nice Sophia-Antipolis (EPU).
- Undergraduate: Angelos Mantzaflaris "Fondements mathématiques 2 (L1 - TD Partie analyse), University of Côte d'Azur, spring semester 2019.

### 8.2.2. Supervision

- PhD in progress: Lorenzo Baldi, Structure of moment problems and applications to polynomial optimization. POEMA Marie Skłodowska-Curie ITN, started in October 2019, supervised by Bernard Mourrain.
- PhD in progress: Ahmed Blidia, New geometric models for the design and computation of complex shapes. ARCADES Marie Skłodowska-Curie ITN, started in September 2016, supervised by Bernard Mourrain.
- PhD in progress: Rima Khouja, Tensor decomposition, best approximations, algorithms and applications. Cotutelle Univ. Liban, started in November 2018, cosupervised by Houssam Khalil and Bernard Mourrain.
- PhD: Ioannis Psarros, Proximity problems for high-dimensional data. Greek scholarships foundation. Defended in Jun. 2019, NKUA, supervised by Ioannis Emiris.
- PhD in progress: Evangelos Bartzos, Algebraic elimination and Distance graphs. ARCADES Marie Skłodowska-Curie ITN, started in June 2016, NKUA, supervised by Ioannis Emiris.

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

- PhD in progress: Apostolos Chalkis, Sampling in high-dimensional convex regions, Google Summer of Code, started in June 2018, NKUA, supervised by Ioannis Emiris.

- PhD in progress: Emmanouil Christoforou, Geometric approximation algorithms for clustering, Structural Bioinformatics national infrastructure "Inspire", started in Jan. 2018, NKUA, supervised by Ioannis Emiris.

- PhD in progress: Tobias Metzlaff. Multivariate orthogonal polynomials and applications to global optimization. POEMA Marie Skłodowska-Curie ITN, started in December 2019, supervised by Evelyne Hubert.

- PhD in progress: Erick Rodriguez Bazan, Symmetry in Algebraic Computations. Inria. Started in November 2017, supervised by Evelyne Hubert.

- PhD : Alvaro Fuentes Suarez defended September 2019 [1]. Modeling shapes with skeletons: scaffolds & anisotropic convolution. ARCADES Marie Skłodowska-Curie ITN, started October 2016 and supervised by Evelyne Hubert.

- PhD in progress: Thomas Laporte, Towards a 4D model of the respiratory system. Fellowship from ED SFA/UCA. Started on October 2019, co-supervised by Benjamin Mouroy (UCA) and Angelos Mantzaflaris.

- PhD in progress: Riccardo Di Dio, Building a diagnosis tool to detect broncho-constrictions, BoostUrCAreer Marie Skłodowska-Curie COFUND fellowship. Started on November 2019, co-supervised by Benjamin Mouroy (UCA) and Angelos Mantzaflaris.

### 8.2.3. *Juries*

Bernard Mourrain was a member of the PhD committee of Matias R. Bender *Algorithms for sparse polynomial systems : Gröbner basis and resultants*, Sorbonne Université, Paris, June 3rd; a reviewer and member of the committee of the HDR of Frédéric Holweck entitled *On the projective geometry of entanglement and contextuality*, University Bourgogne Franche-Comté, Belfort, France, September 11th.

Evelyne Hubert was a reviewer for the Habilitation thesis of Georg Regensbuger, Johannes Kepler University (Austria): *Algebraic and algorithmic Approached to Analysis: Integro-differential equations, positive steady states, and wavelets*

Laurent Busé was a reviewer and member of the committee the PhD thesis of Navid Nemati, *Syzygies: Algebra, Combinatorics and Geometry*, Sorbonne Université, Paris, May 28; he was also a member of the PhD committee of Matias R. Bender, *Algorithms for sparse polynomial systems : Gröbner basis and resultants*, Sorbonne Université, Paris, June 3rd.

## 8.3. Popularization

### 8.3.1. *Interventions*

Ioannis Emiris was an invited speaker at "From Open Access to Science", Athens, May 2019. and "30 years celebration of ATHENA Research Center", Athens, November 2019.

# CARAMBA Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Selection

*10.1.1.1. Member of steering committees*

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

Emmanuel Thomé is a member of the steering committee of the Algorithmic Number Theory Symposium (ANTS).

*10.1.1.2. Member of the Conference Program Committees*

- Aurore Guillevic was a member of the Program Committee of Latincrypt 2019 and WCC 2019.
- Virginie Lallemand was a member of the Program Committee of Asiacrypt 2019.
- Cécile Pierrot was a member of the Program Committee of EUROCRYPT 2020 and Journées Codage et Cryptographie 2020.
- Pierre-Jean Spaenlehauer was a member of the Program Committee of ISSAC 2019.
- Emmanuel Thomé is a member of the scientific directorate of the Dagstuhl computer science seminar series.

### 10.1.2. Journal

*10.1.2.1. Member of the Editorial Boards*

- Virginie Lallemand is a member of the editorial board of the IACR Transactions on Symmetric Cryptology (ToSC) Journal for 2019/2020. This journal is the open-access journal associated to the International Conference on Fast Software Encryption (FSE). She is also a member of the editorial board for the Special Issue of ToSC on Designs for the NIST Lightweight Standardization Process.

*10.1.2.2. 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.

### 10.1.3. Invited Talks

- Cécile Pierrot and Pierrick Gaudry were invited to give a talk at the Elliptic Curve Cryptography Conference (ECC19), Bochum, Germany.
- Marine Minier was invited to give a talk at the Journées Scientifiques Inria in Lyon, France, June 2019.
- Pierrick Gaudry gave a lecture during the Summer School Mathematical foundations of asymmetric cryptography, Aussois, France.
- Aurore Guillevic and Virginie Lallemand were invited to give a talk at the C2 seminar (formerly CCA seminar), Paris, France.
- Aurore Guillevic was invited to give a talk at the Workshop on Randomness and Arithmetics for Cryptography on Hardware in Roscoff, Brittany, France.

### 10.1.4. Research Administration

- Jérémie Detrey chaired the *Commission des Utilisateurs des Moyens Informatiques* (CUMI) of the Inria Nancy – Grand Est research center until November 2019.

- Pierrick Gaudry is:
    - vice-head of the *Commission de mention Informatique* of the *École doctorale IAEM* of the University of Lorraine;
    - a member of the *Conseil Scientifique du GdR IM*;
    - member of the visiting committee for the HCERES evaluation of the CRIStAL laboratory (Lille).
- Aurore Guillevic
    - was member of the CoS, poste MCF number 27MCF1087, Université de Clermont Auvergne;
    - was member of the CoS, poste Chargé d'Enseignement (ChE), École Polytechnique (Palaiseau).
- Marine Minier
    - is a member of Collegium of Science et Techniques of Université de Lorraine;
    - was a member of the CoS, poste MCF number 27MCF-0781944P-4184, Université de Versailles.
- 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 *Comipers* of the Inria Nancy – Grand Est research center, in charge of deciding the attribution of Inria PhD and post-doc grants;
    - is an elected member of the Inria evaluation committee (CE), and a member of the committee "bureau";
    - is an elected member of the Inria technical committee (CTI).
- 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 scientific council of the LIRMM laboratory in Montpellier, France.

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Licence: Jérémie Detrey, *Sécurité des applications Web*, 2h eq. TD, LP, Université de Lorraine, IUT Charlemagne, Nancy, France.

Licence: Pierrick Gaudry, *Intégration Web*, 48h eq. TD, IUT 1A, Université de Lorraine, IUT Charlemagne, 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-lès-Nancy, France.

Master: Marine Minier, *Intégration Méthodologique*, 36h eq. TD, M2 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-Nancy, France.

Master: Marine Minier, *Introduction à la cryptographie*, 15h eq. TD, M1 Informatique, Université de Lorraine, Faculté des sciences et technologies, Vandœuvre-lès-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-lès-Nancy, France.

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

Master: Cécile Pierrot, *Introduction à la cryptographie*, 60h eq. TD, Mastère spécialisé en sécurité, École des Mines de Nancy, France.

Master: Cécile Pierrot, *Introduction à LaTeX*, 6h eq. TD, Master 1, École des Mines de Nancy, France.

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

### *10.2.2. Supervision*

PhD in progress: Sandra Rasoamiaramanana, *Délivrance de contextes sécurisés par des approches hybrides*, since May 2017, PhD CIFRE Orange Gardens, Marine Minier. Planed to be defended in April 2020.

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

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

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

PhD in progress: Hamid Boukerrou, *Design of New Finite State Dynamical Systems Admitting a Matrix Representation: Application to Cryptography*, since Oct. 2019, Marine Minier and Gilles Millerioux.

### *10.2.3. Juries*

Pierrick Gaudry was

- reviewer of the PhD thesis *Arithmétique rapide pour des corps finis* defended by Robin Larrieu, December 2019, École polytechnique;
- member of the PhD thesis jury *Delaunay triangulations of a family of symmetric hyperbolic surfaces in practice* defended by Iordan Iordanov, March 2019, Université de Lorraine;
- member of the HdR jury *Cryptographie basée sur les corps quadratiques : cryptanalyses, primitives et protocoles* defended by Guilhem Castagnos, November 2019, Université de Bordeaux.

Virginie Lallemand was member of the PhD thesis jury: *Optimization of Core Components of Block Ciphers* defended by Baptiste Lambin on the 22nd of October 2019 at the University of Rennes 1.

Marine Minier:

- reviewer of the PhD thesis: Secure Multi-Party Computation and Privacy defended by Aurélien Dupin, June 2019, ENS Ulm, Paris.
- reviewer of the PhD thesis: Optimization of Core Components of Block Ciphers defended by Baptiste Lambin, October 2019, Université de Rennes, Rennes.

- reviewer of the PhD thesis: Représentations adaptées à l'arithmétique modulaire et à la résolution de systèmes flous defended by Jérémie Marrez, December 2019, Université Paris 6, Paris.

- reviewer of the PhD thesis: Security for the Internet of Things: A bottom-up approach to the secure and standardized Internet of Things defended by Timothy Claeys, December 2019, Université Grenoble Alpes, Grenoble.

- President of the PhD thesis jury: Software Datapaths for Multi-Tenant Packet Processing defended by Paul Chaignon, June 2019, Université de Lorraine, Nancy.

- President of the PhD thesis jury: Usability: low tech, high security, defended by Nicolas Blanchard, June 2019, Université de Paris, Paris.

- President of the PhD thesis jury: Contributions à l'analyse de canaux auxiliaires sans connaissance des clairs et chiffrés, et à la recherche de S-boxs compactes, defended by Léo Reynaud, December 2019, Université de Limoges, Limoges.

Emmanuel Thomé was:

- reviewer for the HDR thesis *Algorithmes et implantations efficaces en algèbre linéaire exacte* defended by Pascal Giorgi, October 2019, Université de Montpellier.

- member of the PhD thesis jury *Vote électronique : définitions et techniques d'analyse* defended by Joseph Lallemand, November 2019, Université de Lorraine;

Paul Zimmermann was reviewer of the PhD thesis *Formalisations d'analyses d'erreurs en analyse numérique et en arithmétique à virgule flottante* defended by Florian Faissole, December 2019, Université Paris-Saclay.

## 10.3. Popularization

### 10.3.1. Internal or external Inria responsibilities

Pierrick Gaudry was member of a jury for the Innoviris LAUNCH program, whose goal is to fund start-ups created on the basis of academic work.

### 10.3.2. Articles and contents

- Cécile Pierrot wrote a blog post for Le Monde Binaire.

### 10.3.3. Interventions

- Cécile Pierrot gave a talk about women in science at a meeting *Les Filles, osez les sciences !* in Reims, March 2019.

- Cécile Pierrot and Paul Zimmermann took part in La Fête de la Science, Nancy and Bouxurulles, October 2019.

- Cécile Pierrot gave a talk at La Cité des Sciences, Paris, to open the exhibition called *Espions*, November 2019.

- Pierre-Jean Spaenlehauer gave an introductory talk on polynomial systems to visiting students of the ÉNS Paris-Saclay.

## CASCADE Project-Team

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events Organisation

*8.1.1.1. Events and Activities*

- Quarterly Paris Crypto Days (https://pariscryptoday.github.io) supported by CryptoCloud and aS-CEND

- Seminars are organized: https://crypto.di.ens.fr/web2py/index/seminars

- OPACity – Obfuscation: Proofs, Attacks & Candidates, (http://crypto-events.di.ens.fr/opacity/) Eurocrypt affiliated event. May 19, 2019, Darmstadt, supported by aSCEND

- BibTeX database of papers related to Cryptography, open and widely used by the community (https://cryptobib.di.ens.fr)

*8.1.1.2. Steering Committees of International Conferences*

- Steering committee of CANS: David Pointcheval

- Steering committee of PKC: David Pointcheval

- Steering committee of LATINCRYPT: Michel Abdalla (chair)

- Steering committee of Information-Theoretic Cryptography Conference: Hoeteck Wee

*8.1.1.3. Board of International Organisations*

- Board of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2013 – 2021)

- President-Elect of the *International Association for Cryptologic Research* (IACR): Michel Abdalla (2019 – )

### 8.1.2. Scientific Events Selection

*8.1.2.1. Program Committee Member*

- ACNS '19 (Bogotá, Colombia): Michel Abdalla

- ASIACRYPT '19 (Kobe, Japan): Brice Minaud, Hoeteck Wee

- CT-RSA '19 (San Francisco, California, USA): David Pointcheval

- EUROCRYPT '19 (Darmstadt, Germany): Michel Abdalla

- LATINCRYPT '19 (Santiago, Chile): Michel Abdalla

- PKC '20 (Edinburgh, Scotland): Georg Fuchsbauer

*8.1.2.2. Editorial Boards of Journals*

Editor-in-Chief

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

Associate Editor

- of *ETRI Journal*: Michel Abdalla

- of *Journal of Mathematical Cryptology*: Phong Nguyen

- of *Applicable Algebra in Engineering, Communication and Computing*: David Pointcheval

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

- Master: Michel Abdalla, Brice Minaud, Cryptography, M2, MPRI
- Master: Phong Nguyen, Cryptography, M2, ESIEA
- Bachelor: Brice Minaud, Georg Fuchsbauer, David Pointcheval, Introduction to Cryptology, L3/M1, ENS
- Bachelor: Michel Abdalla, Formal Languages, Computability, and Complexity, L3/M1,
- Bachelor: Georg Fuchsbauer, Cryptography, École supérieure d'ingénieurs Léonard-de-Vinci

### 8.2.2. Defenses

- PhD: Romain Gay, Public-key Encryption, Revisited: Tight Security and Richer Functionalities, ENS, March 18th, 2019 (Supervisors: Michel Abdalla & Hoeteck Wee)
- PhD: Anca Nitulescu, A Tale of SNARKs: Quantum Resilience, Knowledge Extractability and Data Privacy, ENS, April 1st, 2019 (Supervisors: Michel Abdalla, Dario Fiore & David Pointcheval)
- PhD: Razvan Rosie, On the Achievability of White-Box Cryptography, ENS, May 28th, 2019 (Supervisor: Michel Abdalla)
- PhD: Louiza Khati, Full Disk Encryption and Beyond, ENS, July 15th, 2019 (Supervisor: Damien Vergnaud)
- PhD: Jérémy Chotard, Delegation in Functional Encryption, ENS, December 2nd, 2019 (Supervisor: David Pointcheval, with Duong Hieu Phan, at Limoges)

### 8.2.3. Supervision

- PhD in progress: Michele Orrù, Functional Encryption, from 2016, Georg Fuchsbauer & Hoeteck Wee
- 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)
- PhD in progress: Antoine Plouviez, Privacy and Decentralization, from 2018, Georg Fuchsbauer
- PhD in progress: Baptiste Cottier, Privacy-preserving anomaly detection, from 2019, David Pointcheval (with Olivier Blazy, at Limoges)
- PhD in progress: Théo Ryffel, Privacy-preserving federated learning, from 2019, Francis Bach and David Pointcheval
- PhD in progress: Lénaïck Gouriou, Advanced encryption with post-quantum security, from 2019, David Pointcheval (with Cécile Delerablée at Leanear)

### 8.2.4. Committees

- PhD Marc Beunardeau. *Cryptographie Appliquée à la Sécurité des Systèmes d'Information* – Ecole Normale Supérieure – France – January 15th, 2019: David Pointcheval (Chair)
- HdR Catalin Hritcu. *The Quest for Formally Secure Compartmentalizing Compilation* – Ecole Normale Supérieure – France – January 29th, 2019: David Pointcheval
- PhD Romain Gay. *Public-key Encryption, Revisited: Tight Security and Richer Functionalities* – Ecole Normale Supérieure – France – March 18th, 2019: Michel Abdalla and Hoeteck Wee (Co-supervisors)

- PhD Mary Maller. *Practical zero-knowledge arguments from structured reference strings* – University College London – United Kingdom – March 26th, 2019: Georg Fuchsbauer (Reviewer)

- PhD Anca Nitulescu. *A Tale of SNARKs: Quantum Resilience, Knowledge Extractability and Data Privacy* – Ecole Normale Supérieure – France – April 1st, 2019: Michel Abdalla and David Pointcheval (Co-supervisors)

- PhD José Miguel López Becerra. *Provable Security Analysis for the PAKE Problem* – University of Luxembourg – Luxembourg – May 14th, 2019: Michel Abdalla

- PhD Razvan Rosie. *On the Achievability of White-Box Cryptography* – Ecole Normale Supérieure – France – May 28th, 2019: Michel Abdalla (Supervisor)

- HdR Olivier Blazy. *Hash Proofs Systems and Applications to Implicit Cryptography* – Université de Limoges – France – June 12th, 2019: David Pointcheval

- PhD Aurélien Dupin. *Secure Multi-Party Computation and Privacy* – Université Bretagne Loire – France – June 13rd, 2019: David Pointcheval (Co-supervisor)

- PhD Louiza Khati. *Full Disk Encryption and Beyond* – Ecole Normale Supérieure – France – July 15th, 2019: David Pointcheval

- PhD Julian Loss. *New Techniques for the Modular Analysis of Digital Signature Schemes* – Ruhr Universität Bochum – Germany – July 20th, 2019; David Pointcheval (Reviewer)

- PhD Aisling Connolly. *New Notions of Security, Broken Assumptions, and Increased Efficiency* – Ecole Normale Supérieure – France – September 13th, 2019: Michel Abdalla

- PhD Chen Qian. *Lossy Trapdoor Primitives, Zero-Knowledge Proofs and Applications* – Université de Rennes 1 – France – October 4th, 2019: Michel Abdalla

- PhD Alice Pellet–Mary. *On ideal lattices and the GGH13 multilinear map* – Ecole Normale Supérieure de Lyon – France – October 16th, 2019: David Pointcheval (Chair and Reviewer)

- HdR Guilhem Castagnos. *Cryptography based on Quadratic Fields: Cryptanalyses, Primitives and Protocols* – Université de Bordeaux – France – November 8th, 2019: David Pointcheval (Reviewer)

- PhD Joseph Lallemand. *Vote électronique : définitions et techniques d'analyse* – Université de Lorraine – France – November 8th, 2019: David Pointcheval (Reviewer)

- PhD Loïc Ferreira. *Secure Tunnels for Constrained Environments* – Université Bretagne Loire – France – November 18th, 2019: David Pointcheval

- PhD Pauline Bert. *Lattice-based signatures: from construction to implementation* – Université Bretagne Loire – France – November 29th, 2019: David Pointcheval

- PhD Jérémy Chotard. *Delegation in functional encryption* – Université de Limoges - France – Décember 2nd, 2019: David Pointcheval (Co-supervisor) and Michel Abdalla (Chair)

<p style="text-align:center"><span style="color:red">**DATASHAPE Project-Team**</span></p>

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Organisation

- F. Chazal was co-organiser of the Geometric Data Analysis conference at the Stevanovich Center for Financial Mathematics, Chicago, May 2019.
- F. Chazal was co-organiser of the conference New Horizons in Computational Geometry and Topology, Sophia-Antipolis, September 2019.

### 8.1.2. Scientific Events: Selection

*8.1.2.1. Chair of Conference Program Committees*

- Steve Oudot was chair of the program committee for the Young Researchers Forum at the International Symposium on Computational Geometry (SoCG) 2019.

*8.1.2.2. Member of the Conference Program Committees*

- Jean-Daniel Boissonnat was a member of the Organizing Committee of the International Conference on Curves and Surfaces 2019.
- Clément Maria was a member of the Program Committee of the International Symposium on Computational Geometry (SoCG), Portland, USA, June 2019.
- David Cohen-Steiner was a member of the Program Committees of SGP'19 and SMI'19.

### 8.1.3. Journal

*8.1.3.1. 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)*.

Frédéric Chazal is a member of the Scientific Board of Journal of Applied and Computational Topology (Springer).

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

### 8.1.4. Invited Talks

Frédéric Chazal, Geometry of Big Data, Institute of Pure and Applied Mathematics at UCLA, Los Angeles, April 2019.

Frédéric Chazal, Workshop on Data Science, Fundaçao Getulio Vargas, Rio de Janeiro, April 2019.

Frédéric Chazal, SUMTOPO 2019, Topology in Data Science, Johannesburg, June 2019.

Frédéric Chazal, New Horizons in Computational Geometry and Topology, Sophia-Antipolis, September 2019.

Frédéric Chazal, Seminar@System X, Saclay, June 2019.

Clément Maria, Monash University, Australia.

Clément Maria, New Horizons in Computational Geometry and Topology, Sophia-Antipolis, September 2019.

Clément Maria, Applied Algebraic Topology Research Network Seminar, October 2019.

Clément Maria, Dagstuhl Seminar 19352 "Computation in Low-Dimensional Geometry and Topology", August 2019.

Clément Maria, 2ème Demi-journée Pole Calcul - Topologie et Géométrie du Calcul - LIS Marseille, June 2019.

Steve Oudot, Workshop on computational applications of quiver representations: TDA and QPA, Bielefeld University, April 2019.

Steve Oudot, Minisymposium on Algebraic Geometry in Topological Data Analysis, SIAM Conference on Applied Algebraic Geometry, Bern, July 2019.

Steve Oudot, Summer Conference on Topology and its Applications, Johannesburg, July 2019.

Steve Oudot, Spires workshop: from theory to applications of TDA, Oxford, September 2019.

### 8.1.5. 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 is a member of the "Comité de pilotage" of the SIGMA group at SMAI.

Steve Oudot is co-head with Luca Castelli Aleardi (École polytechnique) of the GT GeoAlgo within the GdR-IM.

### 8.1.6. Research Administration

Marc Glisse is president of the CDT at Inria Saclay.

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.

Clément Maria, responsable RAweb pour Datashape.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

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

Master: Marc Glisse and Clément Maria, 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.

Course on TDA at the Statistics with Geometry and Topology Conference 2019, 4hCM, Toulouse, 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, Algorithms for data analysis in C++, 22.5h eq-TD, L3/M1, École polytechnique, France.

### 8.2.2. Supervision

PhD : Alba Chiara de Vitis, Kernel Methods for High Dimensional Data Analysis [12]. Université Côte d'Azur. May 28, 2019. Jean-Daniel Boissonnat and David Cohen-Steiner.

PhD : Sergei Kachanovich, Meshing submanifolds using Coxeter triangulations [11]. Université Côte d'Azur. October 23, 2019. Jean-Daniel Boissonnat.

PhD: Yitchzak Solomon, Inverse problems in topological data analysis, Brown University. Defended in May 2019. Jeff Brock (Yale University) and Steve Oudot.

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: Louis Pujol, Partitionnement de données cytométriques, started Novermber 1st, 2019, Pascal Massart and Marc Glisse.

PhD in progress: Bertrand Beaufils, Méthodes topologiques et apprentissage statistique pour l'actimétrie du piéton à partir de données de mouvement, Frédéric Chazal and Bertrand Michel (Ecole Centrale de Nantes).

PhD in progress: Vincent Divol, statistical aspects of TDA, started September 1st, 2017, Frédéric Chazal and Pascal Massart (LMO).

PhD in progress: Etienne Lasalle, TDA for graph data, started September 1st, 2019, Frédéric Chazal and Pascal Massart (LMO).

PhD in progress: Alex Delalande, Measure embedding with Optimal Transport and applications in Machine Learning, started December 1st, 2019, Frédéric Chazal and Quentin Mérigot (LMO).

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

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. Marco Cuturi (ENSAE & Google Brain) and Steve Oudot.

### 8.2.3. *Juries*

Clément Maria was a member of the jury attributing the Gilles Kahn PhD award, from the SIF and the Academy of Science, Nov. 2019.

Steve Oudot was reviewer and committee member for the PhD defence of Hannah Schreiber, October 2019.

## 8.3. Popularization

### 8.3.1. *Interventions*

- Frédéric Chazal, Un exemple de dispositif dédié aux études cliniques. Seminar on AI, Haute Autorité de Santé, September 2019.

# GAMBLE Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events Organization

*10.1.1.1. Member of the Organizing Committees*

Sylvain Lazard organized with S. Whitesides (Victoria University) the 18th Workshop on Computational Geometry at the Bellairs Research Institute of McGill University in Feb. (1 week workshop on invitation).

Olivier Devillers organized the Trip-Aspag Mini-workshop on routing in triangulations, October 21-25 in Nancy.

### 10.1.2. Scientific Events Selection

*10.1.2.1. Member of the Conference Program Committees*

Guillaume Moroz was in the program committee of the Maple Conference 2019

Xavier Goaoc was on the organizing committee of the Rouen probability meeting

Xavier Goaoc was on the program committee of the Iranian conference on Computational geometry

Xavier Goaoc was on the scientific committee of the Séminaire Francilien de Géométrie Algorithmique et Combinatoire

*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), *Journal of Computational Geometry* (JoCG), *International Journal on Computational Geometry and Applications* (IJCGA), *Journal on Symbolic Computations* (JSC), *SIAM Journal on Computing* (SICOMP), *Mathematics in Computer Science* (MCS), etc.

### 10.1.4. Invited Talks

Olivier Devillers and Monique Teillaud gave talks at the workshop New Horizons in Computational Geometry and Topology

Monique Teillaud gave a talk at the Celebration for the CNRS Silver medal of Claire Mathieu

### 10.1.5. Leadership within the Scientific Community

*10.1.5.1. Steering Committees*

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

### 10.1.6. Research Administration

*10.1.6.1. Hiring committees*

Sylvain Lazard was vice chair of the hiring committee for researchers (CRCN) of Inria Nancy - Grand Est.

Monique Teillaud was a member of the hiring committee for a Professor position at Université Paris Est Marne-la-Vallée.

*10.1.6.2. National committees*

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

*10.1.6.3. 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 is responsible of Fablab of IUT Charlemagne, Univerasité de Lorraine (since 2018, November). Member of *Comité Information Edition Scientifique* of LORIA.

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

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 (since 2018). Head of the Department Algo at LORIA (since 2014). Member of the *Conseil Scientifique* of LORIA (since 2014).

G. Moroz is head of the *Comité des utilisateurs des moyens informatiques* (since nov. 2019). He is member of the CDT, *Commission de développement technologique*, of Inria Nancy - Grand Est (since 2018). He is member of the CLHSCT *Comité local d'hygiène, de sécurité et des conditions de travail* of Inria Nancy - Grand Est (since jan. 2019).

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

M. Teillaud is "Chargée de Mission" as Scientific Advisor for Technologic Development for Inria Nancy-Grand Est. She is a member of the *Conseil de Laboratoire* of LORIA.

*10.1.6.4. 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. Committees

L. Dupont is the secretary of *Commission Pédagogique Nationale Carrières Sociales / Information-Communication / Métiers du Multimédia et de l'Internet* (2017-2022).

L. Dupont: Head of the Bachelor diploma *Licence Professionnelle Animation des Communautés et Réseaux Socionumériques*, Université de Lorraine.

### 10.2.2. Teaching

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

Master: Vincent Despré, *Algorithmique*, 48h, M1, Polytech Nancy, France.

Master: Vincent Despré, *Programmation réseau*, 60h, M1, Polytech Nancy, France.

Master: Vincent Despré, *Architecture avancée*, 20h, M1, Polytech Nancy, France.

Master: Vincent Despré, *Architecture Java EE*, 72h, M1, Polytech Nancy, France.

Licence: Charles Duménil, *Algorithmique et programmation avancée*, 10h, M2, FST, Université de Lorraine, France.

Licence: Charles Duménil, *Découverte de l'informatique*, 88h, L1, Polytech Nancy, Université de Lorraine, France.

Licence: Charles Duménil, *Logiciels scientifiques*, 8h, L3, Polytech Nancy, Université de Lorraine, France.

Licence: Laurent Dupont, *Web development*, 35h, L2, Université de Lorraine, France.

Licence: Laurent Dupont, *Web development*, 150h, L2, Université de Lorraine, France.

Licence: Laurent Dupont *Web development and Social networks* 100h L3, Université de Lorraine, France.

Licence: Xavier Goaoc, *Programmation*, 20 HETD, L3, École des Mines de Nancy, France.

Master: Xavier Goaoc, *Algorithms*, 32 HETD, M1, École des Mines de Nancy, France.

Master: Xavier Goaoc, *Computer architecture*, 32+24 HETD, M1, École des Mines de Nancy + Polytech Nancy, France.

Licence: Galatée Hemery, *Programmation*, 52 HETD, L3, École des Mines de Nancy, France.

Licence: Sylvain Lazard, *Algorithms and Complexity*, 20h, L3, Université de Lorraine, France.

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

### 10.2.3. Supervision

PhD: Iordan Iordanov, Delaunay triangulations of a family of symmetric hyperbolic surfaces in practice, defended March 12th, supervised by Monique Teillaud [11].

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: 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: Nuwan Herath, Fast algorithm for the visualization of surfaces, started in Nov. 2019, supervised by Sylvain Lazard, Guillaume Moroz and Marc Pouget.

### 10.2.4. Juries

M. Teillaud was a member of the PhD committee of Iordan Iordanov (Université de Lorraine)

X. Goaoc was on the reading and defense committees of the habilitation defense of Arnau Padrol (IMJ, Université Paris Sorbonne)

## 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:

Day ♯4 FAN Project, April 23th, Inria project, adult audience.

ISN day, March 7th, adult continuing education of computer science for high-school teachers.

Atelier Google, April 13th, popularization of computer science, general audience.

Atelier Google, December 7th, popularization of computer science, general audience.

<p align="center" style="color:red"><strong>GRACE Project-Team</strong></p>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Selection

*9.1.1.1. Member of the Conference Program Committees*

- Tokenomics 2019, International Conference on Blockchain Economics, Security and Protocols, Paris: D. Augot.
- FAB 2019, Second International Symposium on Foundations and Applications of Blockchain, Los Angeles: D. Augot
- ICBC 2019 (IEEE International Conference on Blockchain and Cryptocurrency, Seoul): D. Augot
- CBT 2019 (3rd International Workshop on Cryptocurrencies and Blockchain Technology, Barcelona)
- ECC 2019 (23rd International Workshop on Elliptic Curve Cryptography, Bochum): B. Smith
- Latincrypt 2019 (Santiago de Chile): B. Smith
- C2SI (*Codes, Cryptographie et Sécurité Informatique*) 2019 (Rabat, Morocco) A. Couvreur

*9.1.1.2. Reviewer*

- Eurocrypt 2019: D. Augot, B. Smith
- Indocrypt 2019 (20th International Conference on Cryptology in India, Hyderabad):D. Augot
- ISIT (International Symposium on Information Theory) 2019: D. Augot, A. Couvreur.
- Latincrypt 2019. A. Couvreur.
- SAC 2019: B. Smith
- STACS 2020: B. Smith

### 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.
- A. Couvreur is member of the editorial board of the *Publications mathématiques de l'Institut de mathématiques de Besançon, Algèbre et Théorie des nombres*.

*9.1.2.2. Reviewer - Reviewing Activities*

- Applicable Algebra in Engineering, Communication, and Computing: B. Smith
- Journal of Cryptographic Engineering: B. Smith
- Journal of Cryptology: B. Smith
- Publications Mathématiques de Besançon: B. Smith
- Transactions on Mathematical Software: B. Smith
- Designs, Codes and Cryptography: A. Couvreur.
- IEEE, Transactions on Information Theory: A. Couvreur.
- IEEE, Transactions on Communication: A. Couvreur.

### 9.1.3. Invited Talks

- D. Augot was invited to the joint Caen-Rouen ArcoCrypt colloquium.

- F. Morain was invited to give a talk at the seminar of the ARIC project-team in Lyon.
- G. Renault was invited to give the main keynote at PHISIC'19 workshop (Gardanne)
- G. Renault was invited to give a talk at the Workshop on Randomness and Arithmetics for Cryptography on Hardware (Roscoff)
- G. Renault was invited to give a talk at the Journée Internationale Post-Quantique organized by Institut Cyber de Grenoble Alpes.
- B. Smith was invited to give a talk at the Workshop on Arithmetic of low-dimensional abelian varieties at ICERM (Providence, USA)
- B. Smith and A. Couvreur were invited to give a talk in the mini-symposium on isogeny-based cryptography at the SIAM Conference on Applied Algebraic Geometry (Bern, Switzerland)
- B. Smith was invited to give a talk in the Autumn session of *Arithmétique en Plat Pays* (Mons, Belgium)
- A. Couvreur was invited speaker at the conference *WCC (Workshop on Coding and Cryptography) 2019* Saint Jacut de la mer, France.
- A. Couvreur was invited speaker at the conference *NuTMIC (Number Theoretic Methods In Cryptography) 2019*, Paris.

### 9.1.4. Seminars

D. Augot is member of the scientific committee of the C2 seminar, which is the French wide, now itinerant, seminar of the subgroup "Codage et Cryptographie" of the CNRS GDR group "Informatique mathématique".

### 9.1.5. Scientific Expertise

G. Renault was member of the Comité d'Évaluation du LJK (Grenoble) pour l'Hcéres.

### 9.1.6. 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); also a member of the board of the Cybersecurity track in the CS Master of IPParis.
- Recruitment committees:
    - D. Augot participated in a selection committee for an Assistant Professor position at École polytechnique.
    - A. Couvreur is member of the *commission scientifique* of Inria Saclay's research centre.
- Funding
    - D. Augot belongs to the Inria-NomadicLabs committee.
    - D. Augot belongs to MATH-INFO subcommittee of Saclay labex Laboratoire Jacques Hadamard, and has been replaced by A. Couvreur.

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

Licence : F. Morain, Lectures for INF361: "Introduction à l'informatique", 15h (equiv TD), 1st year (L3), École polytechnique. Coordinator of this module (350 students).

Licence : B. Smith: *CSE101: Introduction to Computer Programming*, 42h, L1, École polytechnique, France

Licence : G. Renault: INF361, *Introduction à l'informatique*, 50h, L3, École Polytechnique, France.

Master : A. Couvreur : *MPRI 2-13-2: Error Correcting codes and applications to cryptography*.

Master : D. Augot: lectures and labs on crypto in blockchains, 24h, M2, École polytechnique, France.

Master : F. Morain is the scientific leader of the Master of Science and Technology *Cybersecurity: Threats and Defense* of École Polytechnique.

Master : F. Morain and A. Couvreur, INF558, *Introduction to cryptology*, 36h, M1, École Polytechnique.

Master : B. Smith: *INF568: Advanced Cryptography*, 54h, M1, École polytechnique, France

Master : B. Smith and F. Morain: *MPRI 2-12-2: Algorithmes Arithmétiques pour la Cryptologie*, 22.5h, M2, Master Parisien de Recherche en Informatique, France

Master : F. Levy-dit-Vehel, discrete maths, 21h, M1, ENSTA.

Master : F. Levy-dit-Vehel, cryptography, 24h, M2, ENSTA.

### 9.2.2. Supervision

HdR : A. Couvreur, Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique, Paris Diderot University, December 16, 2019.

### 9.2.3. Juries

- D. Augot was member of the thesis committee of Thomas Debris.
- G. Renault was president of the thesis committee of François Boutigny.
- G. Renault was member of the thesis committee of Ramtine Tofighi.
- B. Smith was a member of the thesis committee of Louiza Papachristodoulou (Radboud Universiteit Nijmegen)
- B. Smith was a member of the thesis committee of Joost Renes (Radboud Universiteit Nijmegen)
- B. Smith was a *rapporteur* on the thesis of Yan Bo Ti (University of Auckland).

## 9.3. Popularization

### 9.3.1. Interventions...

- D. Augot was invited to the mathematical colloquium of the University of Besançon.
- Colloque "Blockchains et compétences" à l'Assemblée nationale le 14 mars: D. Augot, who participated to three meetings at Ministry of Finance and Ministry of Industry about blockchains.
- A. Couvreur is *Correspondant de Médiation Scientifique* of Inria Saclay's research centre.
- A. Couvreur organised the *Fête de la science 2019* at Inria Saclay on october 10 and 11 2019. J. Nardi, S. Bordage, M. Chenu de la Morinerie, M. Romeas participated to the event as volunteers.
- A. Couvreur organised the Rendez-vous des Jeunes Mathématiciennes et Informaticiennes (RJMI) at Inria Saclay on october 21 and 22, 2019.

## LFANT Project-Team

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Journal

#### 8.1.1.1. Member of the Editorial Boards

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

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

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

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

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

### 8.1.2. Invited Talks

F. Johansson, *Computing with precision*, Tech Talk, Google X, Mountain View, CA, USA (January 2019)

### 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 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 was a member of the "Conseil National des Universités" (25th section, pure mathematics) since 2015 until november 2019.

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.

He is a member of the administrative council of the Société Arithmétique de Bordeaux, qui édite le *Journal de théorie des nombres de Bordeaux* et qui soutient des congrès en théorie des nombres.

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.

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

Licence: G. Castagnos, *Arithmétique et Cryptologie*, 24h, L3, Université de Bordeaux, France

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

Master: X. Caruso and J.-M. Couveignes, *Algorithmique arithmétique, introduction à l'algorithmique quantique*, 60h, M2, University of Bordeaux, France;

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

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

Licence : J.-P. Cerri, *Arithmétique et Cryptologie*, TD, 36h, L3, Université de Bordeaux, France

Licence : J.-P. Cerri, *Algèbre linéaire*, TD, 51h, L2, Université de Bordeaux, France

Licence : J.-P. Cerri, *Topologie*, TD, 35h, L3, Université de Bordeaux, France

Master : J.-P. Cerri, *Cryptologie*, Cours-TD, 60h, M1, Université de Bordeaux, France

Licence: J. Kieffer, *Algorithmique Mathématique 2*, 32h, L3, Université de Bordeaux, France

Master: R. Barbulescu, *Arithmetic algorithms for cryptology*, M2, Master Parisien de Recherche Informatique.

Licence, Master : J.-P. Cerri, 2 TER (L3, M1), 1 Projet (M2), Université de Bordeaux, France

Master : J. Asuncion, *Elliptic curves*, TD, 16h, M1, Universiteit Utrecht (Mastermath), Pays-Bas

### 8.2.2. Supervision

Master thesis: Jean-Raphaël Biehler, *Functional encryption*, supervised by Guilhem Castagnos

Master thesis: Béranger Seguin, *Deformations of Galois representations*, supervised by Xavier Caruso

Master thesis: William Dallaporta, *Parametrization of ideals and other algebraic structures by quadratic forms*, supervised by Karim 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: Elie Eid, *Computing isogenies between elliptic curves and curves of higher genus*, since September 2018, supervised by Xavier Caruso and Reynald Lercier

PhD in progress: Amaury Durand, *Geometric Gabidulin codes*, since September 2019, supervised by Xavier Caruso

PhD in progress: Jean Kieffer, *Computing isogenies between abelian surfaces*, since September 2018, supervised by Damien Robert and Aurel Page

PhD in progress: Pavel Solomatin *Topics on L-functions*, since October 2014, supervised by B. de Smit and K. Belabas.

PhD in progress: Anne-Edgar Wilke *Enumerating integral orbits of prehomogeneous representations*, since September 2019, supervised by K. Belabas.

PhD in progress: Sudarshan Shinde *Cryptographic applications of modular curves* since October 2016, supervised by R. Barbulescu with Pierre-Vincent Koseleff (Sorbonne Université).

### 8.2.3. Juries

X. Caruso has written a report for the doctoral dissertation by Léo Poyeton, ÉNS de Lyon: *Extensions de Lie $p$-adiques et $(\varphi, \Gamma)$-modules*.

X. Caruso has written a report for the doctoral dissertation by Christopher Doris, University of Bristol: *Aspects of $p$-adic computation*.

X. Caruso has written a report for the doctoral dissertation by Joelle Saade, Université de Limoges: *Méthodes symboliques pour les systèmes différentiels linéaires à singularité irrégulière*.

R. Barbulescu was part of the three members jury of the oral examination in mathematics for math-info the admission examination for ENS de Lyon

D. Robert is a member of the jury of Agregations de Mathematiques. He is also the director of the option "calcul formel" of the Modelisation part of the oral examination.

## 8.3. Popularization

### 8.3.1. Education

Alkindi : R. Barbulescu is one of the three organizers of the Alkindi contest, a contest for 13-to-15 year old students which gathers more than 60000 participants from France and Switzerland. D. Robert and the other members invite the winners of the Bordeaux region for a 2 hour visit each year.

### 8.3.2. Interventions

- from 27/05/2019 to 31/05/2019, X. Caruso supervised a stage at the fablab Coh@bit (at IUT Gradignan) to build some educational material
- 30/06/2019, X. Caruso: *Ramène pas ta science* on a physical experiment demonstrating that the fastest path between two points is an arc of cycloid
- 8-10/10/2019, A. Page: *Fête de la Science* at Inria Bordeaux, activity on cryptography (8 groups of students).
- 17/10/2019, X. Caruso and A. Page: *Village des 80 ans du CNRS*, discussion stand "Quizz des idées reçues" on research in mathematics.
- 19/10/2019, X. Caruso and M.-L. Chabanol: *Village des 80 ans du CNRS* on physical experiment demonstrating that the fastest path between two points is an arc of cycloid
- from 07/04/2019 to 14/04/2019, R. Barbulescu was one of two teachers for a math camp in Kinshasa of 150 students https://www.cnrs.fr/insmi/spip.php?article3190.
- from 06/07/2019 to 13/07/2019, R. Barbulescu was the main organiser for a math training camp which gathered the national teams for the International Olympiad of Mathematics of France, Romania and Bulgaria.
- 5/12/2019, D. Robert: small presentations of cryptography for the student of Ecole Normale Superieure de Lyon.

# OURAGAN Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

#### 10.1.1.1. General Chair, Scientific Chair

- Elias Tsigaridas was the program chair of Mathematical Aspects of Computer and Information Sciences (MACIS 2019), which was held at Istanbul, 13-15 November 2019.

#### 10.1.1.2. Member of the Organizing Committees

A. Quadrat was a member of the organization committee of the *Journées Nationales de Calcul Formel* (JNCF), Luminy, France, 04-08/02/2019. He is now a member of the scientific committee of JNCF.

### 10.1.2. Scientific Events: Selection

#### 10.1.2.1. Member of the Conference Program Committees

Elias Tsigaridas was a program committee member of Computer Algebra in Scientific Computing (CASC 2019).

### 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*
- Alban Quadrat is associate editor of *Multidimensional Systems and Signal Processing*, Springer
- Fabrice Rouillier is a member of the editorial board of *Journal of Symbolic Computation*

### 10.1.4. Leadership within the Scientific Community

Alban Quadrat co-organized the invited sessions *Algebraic and symbolic methods for mathematical systems theory* and *New trends in computational methods for time-delay systems* at the Join *Joint IFAC Conference 7th Symposium on Systems Structure and Control and 15th Workshop on Time Delay Systems*, 9–11 September 2019, Sinaia, Romania

Elias Tsigaridas organized a session on *Algebraic and geometric tools for optimisation and statistics* during the PGMO days 2019, at the EDF'Lab Palaiseau, December 2019.

### 10.1.5. Research Administration

- Alban Quadrat is a member of the Conseil d'Administration of the Société Mathématique de France (SMF).
- Fabrice Rouillier is a member of the scientific commitee of the Indo French Centre for Applied Mathematics.
- Elisha Falbel is director of the "École Doctorale Sciences Mathématiques de Paris Centre - ED 386".

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

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

- Fabrice Rouillier: Course in "Agrégation Option - C", M2, 31 heures, Sorbonne Université
- Antonin Guilloux: Courses and administration of the general math courses in L1 at Sorbonne Université
- Elisha Falbel: First year 'mathématiques approfondie' and master class on Riemann surfaces.
- Pierre-Vincent Koseleff : head of the Master 2 "pr éparation à l'agrégation de mathématiques" at Sorbonne Université.
- Pierre-Vincent Koseleff : Course in M2 "Agrégation de Mathématiques", Computer Algebra, Option C, 100h. Sorbonne Université.
- Pierre-Vincent Koseleff : Course in L3, "algèbre appliquée".

### 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: Grace Younes, 09/2018, directed by Alban Quadrat and Fabrice Rouillier

PhD in progress: Christina Katsamaki, 09/2019, directed by Elias Tsigaridas and Fabrice Rouillier

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

PhD in progress: Raphael Alexandre, 09/2019, directed by Elisha Falbel.

### 10.2.3. Juries

Alban Quadrat was a member of the PhD defense committee of Elisa Hubert, *Surveillance vibratoire d'une transmission de puissance aéronautique*, University of Lyon & Safran Tech, 28/06/2019.

Elisha Falbel was a member of the Habilitation defense committee of Junyan Cao, *Positivité des images directees, extension d'Ohsawa-Takegoshi et applications*, Sorbonne Université , 25/10/2019.

## 10.3. Popularization

- Alban Quadrat co-edited the book *Le Jeu de rôle sur table : un laboratoire de l'imaginaire*, Carrefour des lettres modernes, n. 7, Classiques Garnier, 2019.
- Fabrice Rouillier is a member of the editorial board of *Interstices*
- Fabrice Rouillier is *chargé de mission médiation* at Inria Paris
- Fabrice Rouillier is a member of the *comité de pilotage de l'année des mathématiques*
- Fabrice Rouillier is a member of the *comité de pilotage de la semaine des mathématiques*
- Fabrice Rouillier is the president of the association *Animath*[0]
- Fabrice Rouillier is member of the scientific board of the SMF [0]conference *Mathématiques étonnantes*[0]

### 10.3.1. Internal or external Inria responsibilities

- Alban Quadrat is a member of the technical committee *Linear Systems* of the *International Federation of Automatic Control* (IFAC)
- Elias Tsigaridas is a member of the Evaluation committee (Commission d'Évaluation) of Inria.

### 10.3.2. Interventions

- Fabrice Rouillier participated to the *semaine des mathématiques* for the Paris Inria Paris research center
- Fabrice Rouillier participated to the welcoming of schoolchildren for their *semaine d'observation* at Inria Paris research center.

---

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

[0]Société Mathématique de France

[0]https://smf.emath.fr/actualites-smf/mathematiques-etonnantes-programme

<span style="color:red">**POLSYS Project-Team**</span>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. General Chair, Scientific Chair*

D. Wang was General co-chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019) , Beijing, China, July 15-18, 2019).

*9.1.1.2. Member of the Organizing Committees*

J. Berthomieu was Poster chair of the 44th International Symposium on Symbolic and Algebraic Computation (ISSAC 2019), Beijing, China, July 15-18, 2019).

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Member of the Conference Program Committees*

E. Prouff was member of the program committees of the following conferences:

- Smart Card Research and Advanced Application Conference (CARDIS) 2019
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2019

D. Wang was member of the program committee of the International Symposium on Wen-Tsun Wu's Academic Thought and Mathematics Mechanization (Wu 2019) (Beijing, China, May 12-17, 2019). He was member of the scientific committee of the 4th International Conference on Numerical and Symbolic Computation (SYMCOMP 2019) (Porto, Portugal, April 11-12, 2019).

### 9.1.3. Journal

*9.1.3.1. Member of the Editorial Boards*

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

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

D. Wang is Editor-In-Chief of Mathematics in Computer Science (published by Birkhäuser- Springer, Basel) and member of the Advisory Board for the journal • SCIENCE CHINA Information Sciences (published by Science China Press, Beijing and Springer, Berlin).

D. Wang is member of the Editorial Boards for the Journal of Symbolic Computation (published by Academic Press/Elsevier, London), SN Computer Science (published by Springer Nature, Switzerland) , Texts and Monographs in Symbolic Computation (published by Springer, Wien New York).

D. Wang is member of the International Advisory Board for Communications of JSSAC (Japan Society for Symbolic and Algebraic Computation) (published by JSSAC).

### 9.1.4. Invited Talks

E. Prouff was invited speaker at Spring School on Hardware Security (UK), the NIST Threshold Cryptography Workshop (USA), the Summer School on Real World Crypto and Privacy and the conference on Boolean Functions and Applications (BFA).

M. Safey El Din was invited speaker at the Arctic Applied Algebra conference (Norway), the workshop on Geometry of Real Polynomials, Convexity and Optimization at BIRS Banff International Research Station (Canada), the and the Conference in memory of Wen-tsun Wu's centennial birthday (China).

### 9.1.5. Scientific Expertise

M. Safey El Din was expert for the Czech Republic funding agency.

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

Jérémy Berthomieu had the following teaching activities:

> Master : Polynomial System Solving, 13 hours, M2, Sorbonne Université & Polytech' Sorbonne, France.
> Master : Computation Modeling, 42 hours, M1, Sorbonne Université, France.
> Master : In charge of Basics of Algebraic Algorithms, 50 hours, M1, Sorbonne Université & Polytech' Sorbonne, France.
> Master : Projects supervision, 7 hours, M1, Sorbonne Université, France.
> Licence : Introduction to Cryptology, 15,75 hours, L3, Sorbonne Université , France.
> Licence : Introduction to Numerical Algorithmic, 4,75 hours, L3, Sorbonne Université , France.
> Licence : Introduction to Shell, 38,75 hours, L2, Sorbonne Université , France.
> Licence : Projects supervision, 10 hours, L2, Sorbonne Université, France.

Jean-Charles Faugère had the following teaching activities:

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

Ludovic Perret had the following teaching activities:

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

Mohab Safey El Din has the following teaching activities:

> Master : Polynomial System Solving, 40 hours, M1, Sorbonne Université & Polytech' Sorbonne, 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 : Matías Bender, Algorithms for sparse polynomial systems: Grbner basis and resultants, June 2019, 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 : Olive Chakraborty, Conception and cryptanalysis in secure quantic cryptography, started in May 2017, Jean-Charles Faugère and Ludovic Perret.

#### 9.2.2.1. Juries

E. Prouff was member of the PhD committes of:

- Nicolas Belleville, Université Grenoble Alpes, 21-11-2019, "Compilation pour l'application de contre-mesures contre les attaques par canal auxiliaire"
- Joey Green, Université de Bristol, 20-10-2019, "A Study of Inference-Based Attacks with Neural Networks"
- Aberrahman DAIF, Université Paris 8, 03-05-2019, "Les codes correcteurs au service de la cryptographie symétrique et asymétrique"

J.C. Faugère was member of the PhD committes of:

- Robin Larrieu, École Polytechnique, dec. 2019, "Arithmetique rapide pour des corps finis"

# SECRET Project-Team

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

#### 9.1.1.1. General Chair, Scientific Chair

- FSE 2020, March 2020, Athens, Greece: C. Boura, general chair ; G. Leurent, program co-chair
- PQCrypto 2020, April 15 - April 17, 2020, Paris, France: N. Sendrier, general co-chair ; J.P. Tillich, program co-chair
- Dagstuhl seminar on Quantum Cryptanalysis 2019, October 13-18, 2019, Dagstuhl, Germany: M. Naya-Plasencia co-organizer.

#### 9.1.1.2. Member of the Organizing Committees

- FSE 2019: March 25-28, 2019, Paris, France: Gaëtan Leurent.

### 9.1.2. Scientific Events: Selection

#### 9.1.2.1. Chair of Conference Program Committees

- Co-editor-in-chief of *IACR Transactions on Symmetric Cryptology* starting from 2019: Gaëtan Leurent.
- Co-chair of the Program Committee of *Eurocrypt 2020*, Zagreb, Croatia, May 2020: Anne Canteaut
- Co-chair of the Program Committee of *FSE 2020*, Athens, Greece, March 2020: Gaëtan Leurent.
- Co-chair of the Program Committee of *WCC 2019*, March-April 2019, St Jacut-de-la-Mer, France: A. Canteaut
- Chair of the Program Committee of *QCrypt 2019*, August 26-30 2019, Montreal, Canada: A. Leverrier

#### 9.1.2.2. Member of the Conference Program Committees

- 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, (M. Naya-Plasencia, N. Sendrier, J.P. Tillich);
- CBC 2019: May 18-19, 2019, Darmstadt, Germany, (J.-P. Tillich);
- TQC 2019: June 3-9, 2019, University of Maryland, USA, (A. Chailloux);
- ISIT 2019: July 7-12, 2019, Paris, France, (A. Leverrier, J.-P. Tillich);
- CHES 2019: August 25-28, 2019, Atlanta, USA, (G. Leurent);
- PQC: Perspectives on Quantum Computing, NISQ and beyond: November 20, 2019, Paris, France (A. Leverrier);
- SPACE 2019: December 3-7, 2019, Gandhinagar, India (L. Perrin);
- FSE 2020: March 22-26, 2020, Athens, Greece, (C. Boura, A. Canteaut, G. Leurent co-chair, L. Perrin)
- PQCrypto 2020: April 15-17, 2020, Paris, France (A. Chailloux, M. Naya-Plasencia, N. Sendrier, J.P. Tillich);

- CBCrypto 2020: May 9-10, 2020, Zagreb, Croatia, (J.-P. Tillich);
- Eurocrypt 2020: May 10-14, 2020, Zagreb, Croatia, (A. Canteaut co-chair, M. Naya-Plasencia);
- ISIT 2020: June 21-26, 2020, Los Angeles, USA, (J.-P. Tillich).

## 9.1.3. *Journal*

### 9.1.3.1. *Member of the Editorial Boards*

- *Advances in Mathematics of Communications*, associate editors: N. Sendrier and J.P. Tillich
- *Applicable Algebra in Engineering, Communication and Computing*, associate editor: A. Canteaut.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin.
- *Finite Fields and Applications*, associate editors: A. Canteaut, P. Charpin.
- *IACR Transactions on Symmetric Cryptology*, associate editors: C. Boura, A. Canteaut, G. Leurent (co-editor in chief), M. Naya-Plasencia, L. Perrin.
- *IACR Transactions on Cryptographic Hardware and Embedded Systems*, associate editor: G. Leurent.
- *Quantum (the open journal for quantum science)*, associate editor: A. Leverrier.
- *IEEE Transactions on Information Theory*, associate editor: A. Canteaut.

## 9.1.4. *Invited Talks*

- P. Charpin, *Crooked and weakly crooked functions*, Finite Fields and Applications - Fq14, Vancouver, Canada, June 3-7, 2019.
- M. Naya-Plasencia, *Preparing Symmetric Cryptography for the Quantum World*, FSE 2019, Paris, France, 24-28 March, 2019.

## 9.1.5. *Leadership within the Scientific Community*

- A. Canteaut serves as a chair of the steering committee of *Fast Software Encryption (FSE)*, M. Naya-Plasencia and G. Leurent also serve on the committee.
- 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.

## 9.1.6. *Research Administration*

- A. Canteaut served as Head of Science of the Inria Paris research center until August 2019.
- A. Canteaut serves as Head of *Inria Evaluation Committee* since September 2019.
- P. Charpin serves on the *Comité Parité* at Inria.
- G. Leurent and M. Naya-Plasencia are members of *Inria Paris CSD Committee* (Comité de suivi doctoral).
- M. Naya-Plasencia serves on the *Inria Evaluation Committee* since September 2019.
- A. Leverrier serves on the steering committee of the Domaine D'Intérêt Majeur SIRTEQ (Quantum Technologies in IdF).

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

- 2019 Jury Inria Research Positions (ARP/SRP) (M. Naya-Plasencia);
- 2019 Jury d'admission Inria DR2, (M. Naya-Plasencia);
- 2019 Jury d'admissibilité Inria DR2, (A. Canteaut);
- 2019 Jury d'admissibilité Inria CRCN national (A. Canteaut);
- Committee for the nomination to a permanent position, Radboud University Nijmegen, Netherlands (M. Naya-Plasencia).
- Committee for a professorship in cryptography, TU Graz, Austria (A. Canteaut)

- Reviewer for a promotion to professorhip, ISI Kolkata, India (A. Canteaut)
- Committee for 3 assistant professor positions in computer science at Université de Paris: A. Leverrier

## 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;

Master: A. Chailloux, *Quantum information*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: A. Chailloux, *Quantum algorithms*, 4 hours, M2, Ecole Normale Supérieure de Lyon, France;

Master: A. Leverrier, *Quantum information and quantum cryptography*, 12 hours, M2, University Paris-Diderot (MPRI), France;

Master: L. Perrin, *Application Web et Sécurité*, 24 hours, M1, UVSQ, France;

Bachelor: L. Perrin, *Cryptographie*, 29 hours, L3, UVSQ, France;

Master: J.-P. Tillich, *Introduction to Information Theory*, 36 hours, M2, Ecole Polytechnique, France;

Master: J.-P. Tillich, *Quantum Information and Applications*, 36 hours, M2, Ecole Polytechnique, France.

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

- N. Sendrier, *Code-Based Cryptography*, PQCrypto 2019 Summer School, Chongqing, China, May 6, 2019.

### 9.2.2. Supervision

PhD: Xavier Bonnetain, *Cryptanalysis of symmetric primitives in the post-quantum world*, Sorbonne Université, November 15, 2019, supervisor: M. Naya Plasencia.

PhD: Thomas Debris, *Quantum algorithms for decoding linear codes*, Sorbonne Université, December 17, 2019, supervisor: JP Tillich.

PhD: Antoine Grospellier, *LDPC codes: constructions and decoding*, Sorbonne Université, November 8, 2019, supervisors: A. Leverrier and O. Fawzi (ENS Lyon)

PhD: Vivien Londe, *Study of quantum LDPC codes*, University of Bordeaux, December 6, 2019, supervisors: G. Zémor (Univ. Bordeaux) and A. Leverrier

PhD in progress: Kevin Carrier, *Presque-collisions et applications au décodage générique et à la reconnaissance de codes correcteurs d'erreurs*, since October 2016, supervisor: N. Sendrier and JP Tillich.

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: André Schrottenloher, *Long-term security of symmetric primitives*, since February 2018 supervisor: M. Naya-Plasencia

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.

PhD in progress: Simona Etinski, *Quantum algorithms and protocols*, since October 2019, supervisors: A. Chailloux, A. Leverrier and F. Magniez (Université de Paris)

PhD in progress: A. Florez Gutierrez, *Secure Symmetric Primitives and the Post-Quantum World*, since September 2019, supervisor: M. Naya Plasencia

PhD in progress: Lucien Grouès, *Decoding algorithms for quantum LDPC codes*, since October 2019, supervisors: A. Leverrier, O. Fawzi

PhD in progress: Rocco Mora, *Algebraic structures in code-based cryptography*, since October 2019, supervisor: JP Tillich

## 9.2.3. Juries

- Lorenzo Grassi, *Cryptanalysis of AES-like ciphers and reviving old design ideas for new constructions*, TU Graz, Austria, April 26, 2019, committe: A. Canteaut (reviewer).

- Louiza Khati, *Full Disk Encryption and Beyond*, Université Paris PSL, July 15, 2019, committee: M. Naya-Plasencia (chair).

- T. van Himbeeck, *Quantum Cryptography with Partially Trusted Devices*, Université Libre de Bruxelles, October 18, 2019, committee: A. Leverrier

- A. Aloshious, *Higher dimensional topological codes : structural properties and decoders*, Indian Institute of Technology Madras, November, 2019, committee: J.-P. Tillich (reviewer).

- A. Grospellier, *Décodage des codes expanseurs quantiques et application au calcul quantique tolérant aux fautes*, Sorbonne University, November 8, 2019, committee: A. Leverrier (supervisor), J.-P. Tillich.

- Xavier Bonnetain, *Hidden structures and quantum cryptanalysis*, Sorbonne Université, November 15, 2019, committee: A. Chailloux, M. Naya-Plasencia (Supervisor).

- Loïc Ferreira, *Secure Tunnels for Constrained Environments*, Université Bretagme Loire, November 18, 2019, committee: M. Naya-Plasencia.

- O. Fawzi, HdR, *Contributions to quantum information theory*, École Normale Supérieure de Lyon, December 2, committee: J.-P. Tillich (reviewer).

- V. Londe, *Topological Quantum Error-Correcting Codes beyond dimension 2*, Bordeaux University, December 6, 2019, committee: A. Leverrier (supervisor), JP Tillich

- M. Bozzio, *Security and implementation of advanced quantum cryptography: Quantum money - Quantum weak coin flipping*, Université Paris-Saclay, December 10, 2019, committee: A. Leverrier (reviewer)

- Alain Couvreur, HdR, *Codes algébriques et géométriques, applications à la cryptographie et à l'information quantique*; Université Paris-Diderot, December 16, 2020, committee: N. Sendrier (reviewer), J.P. Tillich

- Patrick Lacharme, HdR, *Études en Securité Informatique*, Université de Normandie, February 6, 2020, committee: M. Naya-Plasencia (reviewer).

- Thomas Debris, *Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse*; Sorbonne Université, December 17, 2019, committee: N. Sendrier, J.P. Tillich (supervisor)

## 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

- *La fragilité inattendue du chiffrement symétrique dans le monde post-quantique*, Gaëtan Leurent and Maria Naya-Plasencia, María, Interstices [63]

### 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, he was also involved in the redaction of the exercises.
- Organization of the event "Rendez-vous des Jeunes Mathématiciennes et Informaticiennes" at Inria Paris (October 28-29) by M. Lequesne, a 2-day camp for 20 high-school girls interested in mathematics and computer science. C. Boura, A. Canteaut and L. Perrin gave talks at this event.
- **Project Algo'scape with a high school (Lycée Anna Judic, Semur en Auxois):** design of an escape game on cryptography (L. Perrin), visit of 15 students at Inria, May 2019 (A. Canteaut and L. Perrin).

<div align="center">

## SPECFUN Project-Team

</div>

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Organisation

*8.1.1.1. General Chair, Scientific Chair*

- Alin Bostan is part of the Scientific advisory board of the conference series *Effective Methods in Algebraic Geometry* (MEGA).
- 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 was until July 2019 elected member (and chair) of the steering committee of the *International Symposium on Symbolic and Algebraic Computation* (ISSAC, 3-year term).
- Georges Gonthier is a member of the steering committee of the *Certified Programs and Proofs* Conference (CPP).

*8.1.1.2. 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 ($\sim 30$ 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 ($\sim 15$ participants per event).

### 8.1.2. Scientific Events: Selection

*8.1.2.1. Member of the Conference Program Committees*

- Alin Bostan and Frédéric Chyzak have served as conference program committee members for the first *Maple Conference*.
- Georges Gonthier has served as a conference program committee members for the first *Workshop on Formal Methods for Blockchains* (FMBC).

*8.1.2.2. Reviewer*

- Frédéric Chyzak has served as reviewer for the selection of the international conferences CICM 2019, ISSAC 2019, and Maple Conference 2019.
- Alin Bostan has served as reviewer for the selection of the international conferences FPSAC 2019 and Maple Conference 2019.

### 8.1.3. Journal

*8.1.3.1. Member of the Editorial Boards*

- Alin Bostan is on the editorial board of the *Journal of Symbolic Computation*.
- Alin Bostan is on the editorial board of the *Annals of Combinatorics*.
- Guy Fayolle is associate editor of the journal *Markov Processes and Related Fields*.
- Georges Gonthier is on the editorial board of the *Journal of Formalized Reasoning*.

*8.1.3.2. Reviewer - Reviewing Activities*

- Alin Bostan has served as a reviewer for the journals: *Journal of Symbolic Computation*, *Journal of Combinatorial Theory, Series A*, *Applicable Algebra in Engineering Communications and Computing*, *Journal of Combinatorial Algebra*, *Annales Henri Lebesgue*, *Annali dell Università di Ferrara*, *Mathematics of Computation*, *Séminaire Lotharingien de Combinatoire*.
- Guy Fayolle has been a reviewer for *Advances in Applied Probability*, *Markov Processes and Related Fields*, *Probability Theory and Related Fields*, *Queueing Systems: Theory and Applications*, *European Journal of Combinatorics*, *Journal of Statistical Physics*, *Physica A*, *Springer Science*.

### 8.1.4. Invited Talks

- Frédéric Chyzak has been invited to give a talk on his joint work with Alin Bostan about the enumeration of walks with small steps in the quarter plane at the international conference Transient Transcendence in Transylvania (Braov, Romania).
- Frédéric Chyzak has been invited to give talks on his joint work with Philippe Dumas about Becker's conjecture on Mahler functions: at the conference Équations Fonctionnelles et Interactions (Anglet), during a Seminar on Symbolic Computation at the Academy of Mathematics and Systems Science, Chinese Academy of Sciences (Beijing, China), and at the conference Differential Galois Theory in Strasbourg (Strasbourg).
- Frédéric Chyzak has been invited to give a talk on his joint work with Alin Bostan, Pierre Lairez, and Bruno Salvy (AriC) at the 6th Summer School in Symbolic Computation (Chongqing, China).
- Alin Bostan has been invited to give a talk at the *Algebraic Marvels in Differential Equations*, Universidade Lisboa, Lisbonne, Portugal, February 2019.
- Alin Bostan has been invited to give a talk at the Combinatorics Seminar, LaBRI, Bordeaux, March 2019.
- Alin Bostan has been a plenary speaker at the international conference AofA 2019, Luminy (France), June 2019.
- Alin Bostan has been a plenary speaker at the international conference FPSAC 2019, Ljubljana (Slovenia), July 2019.
- Alin Bostan has been invited to give a series of five lectures at the Vienna Summer School of Mathematics, Weissensee, Austria, Sept. 2019.

### 8.1.5. Leadership within the Scientific Community

#### 8.1.5.1. Regular Research Seminar

The team organizes a regular seminar, with roughly 10 talks a year. The topics reflect the team's interests: computer algebra, combinatorics, number theory, formal proofs, and related domains.

#### 8.1.5.2. Research Working Group

In 2018, 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, 15 sessions have taken place in 2019.

#### 8.1.5.3. International Conference

Together with Kilian Raschel (CNRS, U. Tours), Alin Bostan co-organized an international conference, Transient Transcendence in Transylvania, held in Romania from May 13 to 17, 2019. They took care together of all the infrastructure for this conference: program, invitations, web page, etc. This conference was a unique event in Romania, with a truly exceptional list of speakers, from several continents and countries: South Africa, Germany, Austria, Canada, United States, France, Netherlands, Poland, and of course, Romania. As a natural continuation of the conference, a volume will be published in the Springer collection PROMS (Proceedings in Mathematics & Statistics), with Bostan and Raschel as editors.

### 8.1.6. Scientific Expertise

- Guy Fayolle is scientific advisor and associate researcher at the *Robotics Laboratory of Mines ParisTech.*
- Georges Gonthier is taking part in an interministerial survey on the technological roadblocks for blockchains, which has been jointly commissioned to Inria, CEA and IMT by the Ministère de l'Economie, the Ministère de l'Education supérieure et de la Recherche, and the Secrétariat d'Etat au Numérique. He also participates to the Blockchain Taskforce set up by the French government.

### 8.1.7. Research Administration

- Frédéric Chyzak is project coordinator of the ANR project *De rerum natura*.
- Guy Fayolle is a member of the working group for *Computer System Modeling* of the *International Federation for Information Processing* (IFIP WG 7.3).
- Georges Gonthier serves on the Conseil de l'École Doctorale de Mathématiques Hadamard.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

**Master**:

Alin Bostan, *Algorithmes efficaces en calcul formel*, 36h, M2, MPRI, France.

Alin Bostan, *Modern Algorithms for Symbolic Summation and Integration*, 21h, M2, Master d'Informatique Fondamentale de l'ENS de Lyon, France.

Frédéric Chyzak, *Algorithmes efficaces en calcul formel*, 22.5h, 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.

### 8.2.2. Juries

- Alin Bostan has served as an examiner in the PhD jury of Robin Larrieu, *Arithmétique rapide pour des corps finis*, Ecole polytechnique, December 10, 2019.
- 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.
- Frédéric Chyzak has served as a reviewer in the PhD jury of Joelle Saade, *Méthodes symboliques pour les systèmes différentiels linéaires à singularité irrégulière*, Université de Limoges, November 5, 2019.
- Frédéric Chyzak has served as a reviewer in the PhD jury of Amélie Trotignon, *Marches sur des réseaux dans des cônes : aspects combinatoires et probabilistes*, Université de Tours, December 6, 2019.
- Pierre Lairez has served as a reviewer in the PhD jury of Josué Tonelli-Cueto, *Condition and Homology in Semialgebraic Geometry*, TU Berlin, November 28, 2019.
- Georges Gonthier has served in the PhD jury of Armaël Guénaud, *Mechanized Verification of the Correctness and Asymptotic Complexity of Programs*, Université de Paris, December 16, 2019.

## 8.3. Popularization

### 8.3.1. Articles and contents

- Georges Gonthier published an interview article *Blockchain: ce que c'est, comment ça marche* in La Recherche, **545**, March 2019.
- Georges Gonthier co-wrote with Ivan Odonnat (Banque de France) *L'avenir du bitcoin et de la blockchain*, in Les Carnets de l'Institut Diderot (2019).

<p style="text-align: center; color: red;">**CAIRN Project-Team**</p>

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Organisation

*8.1.1.1. General Chair, Scientific Chair*

- D. Chillet was the General Co-Chair of HiPEAC RAPIDO'19 Workshop.

*8.1.1.2. Member of the Organizing Committees*

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

### 8.1.2. Scientific Events: Selection

*8.1.2.1. Chair of Conference Program Committees*

- O. Sentieys is Co-Chair of the D8 Track on Architectural and Microarchitectural Design at IEEE/ACM DATE since 2018.
- O. Sentieys is a member of the committee for delivering the Best Paper Award at IEEE/ACM DATE 2020.
- O. Sentieys served as a committee member in the IEEE EDAA Outstanding Dissertations Award (ODA).

*8.1.2.2. 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'19, IEEE FPT'19, IEEE ASAP'19 and ARC'19.
- A. Kritikakou was a member of technical program committee of IEEE RTAS'20, ECRTS'19, SAMOS'19, DATE'20.
- O. Sentieys was a member of technical program committee of IEEE/ACM DATE, IEEE FPL, ACM ENSSys, ACM SBCCI, IEEE ReConFig.
- T. Yuki was a member of technical program committee of CGO '19, SC '19, TAPAS '19, CC '20, IMPACT '20, and was a member of external review committee of PACT '19.

### 8.1.3. Journal

*8.1.3.1. Member of the Editorial Boards*

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

### 8.1.4. Invited Talks

- O. Sentieys gave an invited talk at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Louvain-la-Neuve, Belgique, January 2019 on "Approximating Deep Learning Accelerators".
- O. Sentieys gave an invited talk at ARCHI Spring School, Lorient, France, May 2019 on "Design of VLSI Integrated Circuits - A (very) deep dive into computing chips".

- O. Sentieys gave a Keynote at the IEEE International Nanodevices and Computing (INC) - IEEE International Conference on Rebooting Computing (ICRC), Grenoble, France, April 2019 on "Playing with numbers for Energy Efficiency: Introduction to Approximate Computing" [21].
- O. Sentieys gave a tutorial at the 22nd IEEE/ACM Design, Automation and Test in Europe (DATE), March 2019 on "A Comprehensive Analysis of Approximate Computing Techniques: From Component- to Application-Level" [47].
- D.Chillet gave a talk during GDR SoC2 and RO topic day, in november 2019 on "Mathematics model for wavelength allocation in the context of Optical NoC".
- D. Chillet gave an invited talk at FETCH (École d'hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes), Louvain-la-Neuve, Belgique, January 2019 on "Power management for communications on Optical NoC".

### 8.1.5. 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 a member of the French National University Council in Signal Processing and Electronics (CNU - Conseil National des Universites, 61ème section) since 2019.
- D. Chillet is member of the Board of Directors of Gretsi Association.
- D. Chillet is co-animator of the "Connected Objects" topic 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 GDR SoC$^2$.
- O. Sentieys is an elected member of the Evaluation Committee (CE) of Inria.

### 8.1.6. Scientific Expertise

- O. Sentieys served as an expert for Fund for Scientific Research – FNRS, Belgium.
- D.Chillet served as an expert for the call CAPES-COFECUB 2020.
- D.Chillet served as an expert for German Research Foundation.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching Responsibilities

- E. Casseau is in charge of the Department of "Digital Systems" at ENSSAT Engineering Graduate School.
- D. Chillet was the responsible of the ICT Master of University of Science and Technology of Hanoi.
- C. Killian was the responsible of the second year of the "Instrumentation" DUT at IUT, Lannion until July 2019.
- O. Sentieys is responsible of the "Embedded Systems" major of the SISEA Master by Research.
- C. Wolinski was the Director of ESIR until May 2019.

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.

### 8.2.2. 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)

S.I. Filip, Operating Systems, 24h, Master of Mechatronics, ENS RENNES (M2)

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

F. Charot: Computer architecture, 58h, ISTIC (L3)

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

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

D. Chillet: advanced processor architectures, 20h, ENSSAT (M2)

D. Chillet: micro-controller, 64h, ENSSAT (L3)

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

D. Chillet: low-power digital CMOS circuits, 4h, UBO (M2)

C. Killian: digital electronics, 52h, IUT Lannion (L1)

C. Killian: automated measurements, 44h, 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, 60h, ISTIC (L3)

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)

### 8.2.3. Supervision

PhD: Audrey Lucas, Software support resistant to passive and active attacks for asymmetric cryptography on (very) small computation cores, Dec. 2019, A. Tisserand.

PhD: Genevieve Ndour, Approximate computing for high energy-efficiency in internet-of-things applications, Jul. 2019, A. Tisserand, A. Molnos (CEA LETI).

PhD in progress: Thibault Allenet, Low-Cost Neural Network Algorithms and Implementations for Temporal Sequence Processing, March 2019, O. Sentieys, O. Bichler (CEA LIST).

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: Corentin Ferry, Compiler support for Runtime data compression for FPGA accelerators, Sep. 2019, S. Derrien, T. Yuki and S. Rajopadhye (co-tutelle between Université de Rennes 1 and Colorado State University).

PhD in progress: Adrien Gaonac'h, Test de robustesse des systèmes embarqués par perturbation contrôlée en simulation à partir de plateformes virtuelles, Oct. 2019, D. Chillet, Yves Lhuillier (CEA LIST), Youri Helen (DGA).

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

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: Louis Narmour, Revisiting memory allocation in tyeh polyhedral model, Sep. 2019, S. Derrien, T. Yuki and S. Rajopadhye (co-tutelle between Université de Rennes 1 and Colorado State University).

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 (IRISA/GRANIT).

## 8.3. Popularization

### 8.3.1. Articles and contents

O. Sentieys contributed to the Inria white book on scientific reviews and challenges in cybersecurity https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf.

### 8.3.2. Interventions

Members of the team participated in the national science festival *(Fête de la Science)* in Lannion, October, with demonstrations on wireless sensor networks, body sensor network, cryptology and digital circuit design.

# CAMUS Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

#### 10.1.1.1. Member of the Organizing Committees

Philippe Clauss organized the Special Session on Compiler Architecture, Design and Optimization (CADO) of the 17th International Conference on High Performance Computing & Simulation (HPCS 2019), July 2019, Dublin, Ireland.

Philippe Clauss will organize the 10th edition of the International Workshop on Polyhedral Compilation Techniques, held in conjunction with HiPEAC 2020, January 22, 2020, Bologna, Italy.

Cédric Bastoul co-organized HIP3ES 2019 (International Workshop on High Performance Energy Efficient Embedded Systems), in conjunction with the international conference HiPEAC 2019.

Arthur Charguéraud co-organized the summer school École des Jeunes Chercheurs en Programmation (EJCP), June 2019, Strasbourg, France.

### 10.1.2. Scientific Events: Selection

#### 10.1.2.1. Member of the Conference Program Committees

Vincent Loechner has been member of the program committees of HIP3ES 2019, PDP 2020, IMPACT 2020.

Philippe Clauss has been part of the program committees of: CC 2020 (ACM SIGPLAN International Conference on Compiler Construction); ICPP 2020 (49th International Conference on Parallel Processing); IPDRM 2019 (Third Annual Workshop on Emerging Parallel and Distributed Runtime Systems and Middleware, held in conjunction with the International Conference for High Performance Computing, Networking, Storage and Analysis, SC 19).

Arthur Charguéraud has been member of the program committees of ITP 2019, POPL 2020, OOPSLA 2019.

Cédric Bastoul has been part of the program committee of HiPC 2019 (IEEE International Conference on High Performance Computing, Data and Analytics), HIP3ES 2019 (International Workshop on High Performance Energy Efficient Embedded Systems), IMPACT 2019 (International Workshop on Polyhedral Compilation Techniques), CADO 2019 (Special Session on Compiler Architecture, Design and Optimization of the 17th International Conference on High Performance Computing & Simulation - HPCS 2019).

#### 10.1.2.2. Reviewer

Bérenger Bramas has been a reviewer for COMPAS 2019 and PDP 2020.

Arthur Charguéraud has been a reviewer for FOSSACS 2020 and ESOP 2020.

### 10.1.3. Journal

#### 10.1.3.1. Member of the Editorial Boards

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

#### 10.1.3.2. Reviewer - Reviewing Activities

Bérenger Bramas has been a reviewer for the following journals: Journal of Parallel Computing (Elsevier), Journal of Parallel and Distributed Computing (Elsevier), Journal of Computer Science and Technology (Springer), Parallel Processing Letters (World Scientific), Software: Practice and Experience (Wiley).

Philippe Clauss has been a reviewer for the Journal of Software: Practice and Experience (Wiley).

### 10.1.4. Invited Talks

Cédric Bastoul delivered the invited talk "Loop Optimization: A Matter of Art and Science" at the Huawei Symposium on Foundations of Software 2019.

### 10.1.5. Scientific Expertise

*10.1.5.1. Standardization*

Since Nov. 2014, Jens Gustedt has been a member of the ISO working group SC22-WG14 for the standardization of the C programming language and serves as a co-editor of the standards document, see [46], [47], [40], [33]. He participates actively in the clarification report processing, the planning of future versions of the standard and in a subgroup that discusses the improvement of the C memory model, see [45], [35], [48].

He was one of the main forces behind the elaboration of C17, the new version of the C standard that has been published by ISO in 2018 [51] and contributes to the future standard "C2x" in various ways. In particular he proposed the removal of the so-called K&R definitions [27], the reform of sign representation [25], [26], maximum width integers [44], keywords [31], [41], [36], [36], null pointer constants [34], timing interfaces [37], [30], [30], atomicity and synchronization [42], [32], [39], and function error conventions [28]. Most of these are either integrated in the latest draft or have been adopted subject to reformulations and adaptations.

*10.1.5.2. Expertise*

Philippe Clauss has been a reviewer for a promotion case to Full Professor in a US University.

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

### 10.1.6. Research Administration

Cédric Bastoul, Philippe Clauss and Vincent Loechner are members of the *Comité d'Experts (section 27, informatique)* of the Université de Strasbourg, providing their scientific and teaching expertise to the university and to the academy. In particular, this committee is involved in the recruitment of researchers and teachers in computer science. Philippe Clauss has been the Vice President of the committee since April 2019.

Jens Gustedt is the head of the ICPS team for the ICube lab, and in that function a member of the board of directors of the lab. He is also a member of the local recruitment committee for PhD students and postdocs of 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 Inria Center Nancy — Grand Est. This group of scientists provides scientific expertise to the Director of the Center.

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Master: Bérenger Bramas, Compilation and Performance, 39h, M2, Université de Strasbourg, France

Master: Bérenger Bramas, Compilation, 30h, M1, Université de Strasbourg, France

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

Licence: Vincent Loechner, algorithmique et programmation, 168h, L1, Université de Strasbourg, France

Licence: Vincent Loechner, administration système et internet, 45h, L3, Université de Strasbourg, France

Licence: Vincent Loechner, programmation parallèle, 23h, L3, Université de Strasbourg, France

Master: Vincent Loechner, programmation temps réel, 10h, M2, Université de Strasbourg, France

Master: Vincent Loechner, calcul parallèle, 20h, 3ième année école d'ingénieur (TPS), Université de Strasbourg, France

Licence: Philippe Clauss, Computer architecture, 18h, L2, Université de Strasbourg, France

Licence: Philippe Clauss, Bases of computer architecture, 22h, L1, Université de Strasbourg, France

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

Master: Philippe Clauss, Real-time programming and system, 37h, M1, Université de Strasbourg, France

Master: Philippe Clauss, Code optimization and transformation, 31h, M1, Université de Strasbourg, France

Licence (Math-Info): Alain Ketterlin, Algorithmique et programmation, L1, 96h, Université de Strasbourg, France

Licence (Math-Info): Alain Ketterlin, Architecture des systèmes d'exploitation, L3, 38h, Université de Strasbourg, France

Licence (Math-Info): Alain Ketterlin, Programmation système, L2, 40h, Université de Strasbourg, France

Master (Informatique): Alain Ketterlin, Preuves assistées par ordinateur, 18h, Université de Strasbourg, France

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

Licence: Éric Violard, Programmation fonctionnelle, 162h, L1, Université de Strasbourg, France

Licence: Éric Violard, Bases de l'architecture informatique, 62h, L1, Université de Strasbourg, France

Licence: Éric Violard, Architecture des ordinateurs, 45h, L2, Université de Strasbourg, France

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

Licence: Cédric Bastoul, Computer architecture, 78h, L1, Université de Strasbourg, France, and 25h, L1, UFAZ Azerbaijani-French University, Azerbaijan

Licence: Cédric Bastoul, Parallel programming, 20h, L3, Université de Strasbourg, France, and 25h, L3, UFAZ Azerbaijani-French University, Azerbaijan

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

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

Master: Cédric Bastoul, Introduction to Research, 3h, L2+M1, Université de Strasbourg, France

### 10.2.2. Supervision

PhD: Armaël Géneau, *Formal verification of complexity analyses*, co-advised by Arthur Charguéraud and François Pottier, defended on December 16th, 2019.

PhD: Paul Godard, *Parallélisation et passage à l'échelle durable d'une chaîne de traitement graphique pour l'impression professionnelle*, Université de Strasbourg, Dec. 16, 2019. Cédric Bastoul and Vincent Loechner.

PhD: Maxime Schmitt, *Génération automatique de codes adaptatifs*, Université de Strasbourg, Sept. 30, 2019. Cédric Bastoul and Philippe Helluy.

PhD: Daniel Salas, *Parallélisation hybride d'une application de détection de noyaux cellulaires*, Université de Strasbourg, Sept. 10, 2019. Jens Gustedt.

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

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

### 10.2.3. Juries

Philippe Clauss participated in the following PhD committees in 2019:

| Date | Candidate | Place | Role |
|------|-----------|-------|------|
| Jan. 28 | Hugo Brunie | Université de Bordeaux | Reviewer |
| Oct. 25 | Ksander EJJAAOUANI | Université de Strasbourg | President |
| Dec. 9 | Arif Ali ANAPPARAKKAL | Université de Rennes | Examiner |
| Dec. 19 | Hang YU | Université Grenoble Alpes | Reviewer |

Cédric Bastoul participated in the following PhD committees in 2019:

| Date | Candidate | Place | Role |
|------|-----------|-------|------|
| Mar. 29 | Pierre Huchant | Université de Bordeaux | Reviewer |
| Jun. 21 | Chandan Reddy | École Normale Supérieure | Reviewer |

## 10.3. Popularization

- 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 than 700,000 teenagers played with the interactive exercises in November 2019. More information on: http://castor-informatique.fr/.

### 10.3.1. Articles and contents

- Jens Gustedt authored the book *Modern C* [24], which since the first publication of an online draft in 2016 has become one of the major references for the C programming language.

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

### 10.3.2. Education

- Cédric Bastoul participated in the training of high school teachers involved in the forthcoming optional Computer Science course for high school students. Specifically, he produced lectures and materials to teach Computer Architecture to high school students.

### 10.3.3. Interventions

- Vincent Loechner has been organizing a hub for the Google Hashcode programming contest (online qualification round) at Université de Strasbourg in Feb. 2019. More than 30 students and colleagues were hosted in the university classrooms to participate to this event.

- Cédric Bastoul delivered a presentation on program optimization at "Journée des licences" ("Bachelor Day") in June 2019.

### 10.3.4. Internal action

- Bérenger Bramas, Jens Gustedt and other members of the scientific computing group (*axe transverse calcul scientifique*) organized two software corners at the ICube laboratory. A software corner is a meeting where researchers exchange about programming best practices, existing and upcoming tools, and their own experiences.

<h1 style="text-align:center; color:red">CASH Project-Team</h1>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. Member of the Organizing Committees*

- Laure Gonnord animates the french compilation community since 2010 (http://compilfr.ens-lyon.fr.

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Chair of Conference Program Committees*

- Laure Gonnord was PC chair and organizer of the 8th Numerical and Symbolic Abstract Domain (NSAD, satellites workshop of SAS 2019, FM2019, in Porto.)
- Ludovic Henrio was chair of the ICE'19 workshop.

*9.1.2.2. Member of the Conference Program Committees*

- Laure Gonnord is a PC member of **CAV** 2019 Conference on Computer-Aided Verification. She will be PC member of SBLP'20 (Brazilian Symposium on Programming Languages).
- Ludovic Henrio has been a PC member of FASE 2019, ACSD 2019, Coordination 2019, HLPP 2019, AGERE 2019, and iFM 2019
- Christophe Alias has been a PC member of COMPAS'19.

*9.1.2.3. Reviewer*

- Christophe Alias was reviewer for MCSoC'19.
- Matthieu Moy was reviewer for CAV'19, IFM'19, MCSOC'19

### 9.1.3. Journal

*9.1.3.1. Reviewer - Reviewing Activities*

- Ludovic Henrio was reviewer for the HLPP'19 special issue in IJPP. He is also guest editor for the special issues associated to the ICE workshop of the last 4 years.
- Christophe Alias was reviewer for ACM TOPC.
- Matthieu Moy was reviewer for Journal of Electronics.

### 9.1.4. Invited Talks

- Matthieu Moy presented a talk "La génération de code temps réel sur architecture many-coeur" at the annual colloquium of GDR SOC2.

### 9.1.5. Research Administration

- Laure Gonnord is elected member of the LIP council and the Fédération d'Informatique de Lyon council.
- Laure Gonnord is elected member of the Inria National "Commission d'Evaluation" from september 2019.

## 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, TD+TP, 42h, L2, UCBL
- Laure Gonnord, Operating Systems, TD+TP, 26h, L2, UCBL
- Matthieu Moy, Concurrent Programming, CM+TD+TP, 57h, L3, UCBL.
- Matthieu Moy, Recursive Programming, TD+TP, 48h, L1, UCBL.
- Matthieu Moy, Git, CM+TP: 12h, L3, UCBL.
- Amaury Maillé, Concurrent Programming, 8h TD, 14 h 30 TP, L3, UCBL.
- Paul Iannetta, ACM, TD, 32h, L3, ENS de Lyon.
- Paul Iannetta, Projet 1, TD, 36h, L3, ENS de Lyon.
- Paul Iannetta, Colloquium L3, TD, 2h, L3, ENS de Lyon
- Paul Iannetta, Jury de stage, TD, 4h, L3, ENS de Lyon
- Julien Braine, ASR, TP et TD, 32h, L3, ENS de Lyon.

Master:

- Christophe Alias, Compiler optimizations for embedded applications, CM+TD, 27h, 4A, INSA Centre Val de Loire.
- Laure Gonnord, Compilation and Program Analysis, CM, 10h, TP 8h, 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, Distributed Systems, TD 9h, M1, UCBL.
- Laure Gonnord, Graphs, Complexity, Algorithmics, M1 MEEF (CAPES Maths, prepa), CM+TD+TP+oral training, 18h, UCBL.
- Laure Gonnord, Algorithmics, Systems M1 MEEF (CAPES NSI, prepa), CM+TD, 15h, UCBL.
- Laure Gonnord, Algorithmics, Architecture, Systems, DIU EIL, CM+TD+TP, 60h, UCBL.
- Matthieu Moy, Software Engineering, CM+TD+TP, 25h, M1, UCBL.
- Matthieu Moy, Compilation and Program Analysis, TP, 16h, M1, ENS de Lyon.
- Matthieu Moy, Compilation and program transformations, TD+TP, 25h, M1, UCBL.
- Ludovic Henrio, Compilation and Program Analysis, CM, 10h; TP, 6h, M1, ENS de Lyon.
- Ludovic Henrio, Distributed Systems: an algorithmic approach, CM+TD, 3h, M2 Specialite IFI (Ingénierie et Fondements de l'Informatique), parcours CSSR, and UBINET, Université de Nice Sophia-Antipolis.
- Amaury Maillé, Networks, 2h TD, M1, UCBL.
- Paul Iannetta, Projet Intégré, TD, 14h, M1, ENS de Lyon.
- Paul Iannetta, Jury de stage, TD, 4h, M1, ENS de Lyon
- Julien Braine, APPD, TP et TD, 28h, M1, ENS de Lyon.

### 9.2.2. Supervision

- 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: 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).

- PhD in progress: Amaury Maillé, "Programming model to assemble compute kernels safely and efficiently: Future- based synchronization for arrays and matrices", ENS Lyon, supervised by Matthieu Moy and Ludovic Henrio. Started in October 2019, supervised by Gaëtan Hains (Huawei), Wijnand Suijlen (Huawei), Françoise Baude (UNS./I3S), Ludovic Henrio (LIP).

### 9.2.3. Juries

- Laure Gonnord was external jury member for the PhD of Yohan Uguen, "High-level synthesis and arithmetic optimizations" (INSA de Lyon).

- Ludovic Henrio was part of the reading commitee of Keyvan Azadbakht (Universiteit Leiden).

- Christophe Alias was a reviewer and member of the PhD committee of Hang YU (Université Grenoble-Alpes).

- Christophe Alias was *correcteur* and jury member for *concours d'admission X/ENS*.

- Laure Gonnord was jury member for the *C*oncours d'admission de l'Agrégation de Sciences Industrielles, spécialité Informatique Industrielle, in June 2019.

- Matthieu Moy was reviewer for the Ph.D of Hamza Deroui, "Étude et implantation d'algorithmes pour l'ordonnancement d'applications dataflow" (INSA Rennes).

## 9.3. Popularization

### 9.3.1. Articles and contents

- "Pourquoi créer des nouveaux langages de programmation?" Ludovic Henrio. Interstices. Janvier 2019.

### 9.3.2. Education

- Laure Gonnord has participated to the construction of the diploma "teaching computer science in high schools" in Lyon, and also the new preparatory cursus for the "CAPES-NSI" at Lyon1 university.

### 9.3.3. Interventions

- Laure Gonnord was invited by the "Association des profs de Prepa" to give her expertise about teaching computer science in the first universitary cycle. The context is the creation of a new preparatory class with a computer science minor "MPI" (Maths, Physics, Computer Science).

- Matthieu Moy presented a talk "Se lancer dans le logiciel libre quand on est étudiant (ou pas)" at "Campus du libre", Lyon.

<p style="text-align:center"><span style="color:red">**CORSE Project-Team**</span></p>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. Member of the Organizing Committees*

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

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Member of the Conference Program Committees*

- Frédéric Desprez: IPDPS, HPC, CCGRID, ParCo, ICA3PP, CloudCom
- François Broquedis: IPDPS, COMPAS
- Fabrice Rastello: ACM SIGPLAN/SIGBED LCTES 2019; IEEE/ACM SIGPLAN CGO 2020; IEEE/ACM SIGARCH PACT 2019; CADO 2019
- Yliès Falcone: AFADL'19, SHPCS'19, IFIP-ICTSS'19, RV'19, FDL'19, 4PAD'19, TASE'19, SAC-SVT'19
- Manuel Selva: ReCoSoC'19

### 9.1.3. Journal

*9.1.3.1. Member of the Editorial Boards*

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

*9.1.3.2. Reviewer - Reviewing Activities*

- Frédéric Desprez: ACM Transactions on Internet of Things, IEEE Access
- Fabrice Rastello: ACM TACO, ACM TOPLAS

### 9.1.4. 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

### 9.1.5. Scientific Expertise

- Frédéric Desprez: Genci: attribution heures de calcul CT6
- Frédéric Desprez: Groupe de travail "Cloud pour l'IA" d'Allistène
- Frédéric Desprez: Comité des sages IRIT
- Yliès Falcone: Review for ANR call for projects

### 9.1.6. Research Administration

- Frédéric Desprez: Deputy Scientific Director at INRIA
- Frédéric Desprez: Director of the GIS GRID5000
- Frédéric Desprez: Conseil Scientifique ESIEE Paris
- Frédéric Desprez: Groupe de travail "Infrastructures" Inria

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

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

License 3: François Broquedis, Introduction to UNIX, 20 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, 30 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, Object-Oriented Programming, 20 hours, Grenoble Institute of Technology (Ensimag)

François Broquedis is in responsible of the first year of Ensimag

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

Licence: Florent Bouchez Tichadou, Algorithms languages and programming, 160 hours, L2 UGA

Licence: Florent Bouchez Tichadou was responsible of the second year (L2) of INF (informatique) and MIN (mathématiques et informatique) students at UGA from January to June, eq. 42 hours

Licence: Florent Bouchez Tichadou, Software Project, 10 hours, L3 UGA

Data Asperger, Florent Bouchez Tichadou, Formation d'autistes Asperger aux métiers du développement informatique et analyse des données. Bloc Algorithmique. 20 hours, GEM & Le Campus Numérique.

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, was co-responsible of the first year of the International Master of Computer Science (Univ. Grenoble Alpes and INP ENSIMAG) until August 2019.

License 3: Manuel Selva, Imperative programming using python, 60 hours, Grenoble Institute of Technology (Ensimag)

License 3: Manuel Selva, Introduction to UNIX, 15 hours, Grenoble Institute of Technology (Ensimag)

Master 1: Manuel Selva, Operating systems and concurrent programming, 15 hours, Grenoble Institute of Technology (Ensimag)

### 9.2.2. Supervision

PhD: Georgios Christodoulis, Adaptation of a heterogeneous run-time system to efficiently exploit FPGA, December 5, 2019, 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: Fabian Grüber, Performance Debugging Toolbox for Binaries: Sensitivity Analysis and Dependence Profiling, December 17 2019, advised by Fabrice Rastello

PhD: Raphaël Jakse, Interactive Runtime Verification, December 18 2019, advised by Jean-François Méhaut and Yliès Falcone.

PhD in progress: Auguste Olivry, Data Locality and Parallelism Optimization for Linear and Multilinear Algebra, September 2019, advised by Fabrice Rastello.

PhD in progress: Nicolas Tollenaere, Optimizing ML algorithms for MPPA Asics, April 2019, advised by Fabrice Rastello.

PhD in progress: Nicolas Derumigny, Automatic generation of performance models for heterogeneous architectures, September 2019, advised by Fabrice Rastello.

PhD in progress: Théo Barollet, Problem-based learning: automatic generation and recommendation of programming exercises, September 2019, advised by Florent Bouchez Tichadou and Fabrice Rastello.

### 9.2.3. *Juries*

#### 9.2.3.1. *Fabrice Rastello*

Fabian Grüber, advisor, *Performance Debugging Toolbox for Binaries: Sensitivity Analysis and Dependence Profiling*, PhD, Université Grenoble Alpes, December 17 2019

Maxime Schmitt, reviewer, *Automatic Generation of Adaptative Codes*, PhD, Université de Strasbourg, September 30 2019

#### 9.2.3.2. *Frédéric Desprez*

Michael Mercier, examiner, *Contribution to High Performance Computing and Big Data Infrastructure Convergence*, PhD, Université Grenoble Alpes, January 07 2019

Alexandre Veith, examiner, *Quality of Service Aware Mechanisms for (Re)Configuring Data Stream Processing Applications on Highly Distributed Infrastructure*, PhD, Lyon, September 23 2019

Nathanaël Cheriere, reviewer, *Towards Malleable Distributed Storage Systems From Models to Practice*, PhD, Ecole normale supérieure de Rennes, November 5 2019

Ayham Kassab, reviewer/president, *Optimisation de l'ordonnancement de calculs parallèles et de l'engagement de sources d'énergie renouvelable pour l'alimentation des centres de calcul*, PhD, Université de Bourgogne Franche Comté, November 14 2019

Georgios Christodoulis, advisor, *Adaptation of a heterogeneous run-time system to efficiently exploit FPGA*, PhD, Université Grenoble Alpes, December 5, 2019

#### 9.2.3.3. *François Broquedis*

- Georgios Christodoulis, advisor, *Adaptation of a heterogeneous run-time system to efficiently exploit FPGA*, PhD, Université Grenoble Alpes, December 5, 2019

#### 9.2.3.4. *Yliès Falcone*

- Raphaël Jakse, advisor, *Interactive Runtime Verification*, PhD, Université Grenoble Alpes, December 18 2019.

## 9.3. Popularization

### 9.3.1. *Education*

DIU EIL, Florent Bouchez Tichadou, Formation des enseignants des lycées suite à la réforme du Bac et l'introduction de l'option informatique en 1ère et Terminale (NSI). Bloc algorithmique par Apprentissage Par Problèmes (APP). Académie de Grenoble ainsi que les enseignants dans les lycées français à l'étranger.

<p style="text-align:center; color:red"><strong>PACAP Project-Team</strong></p>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Selection

*10.1.1.1. Member of the Conference Program Committees*

- Caroline Collange is a member of the program committee of the DATE 2020 conference
- Pierre Michaud was a member of the program committee of the International Conference on Computer Design (ICCD 2019)
- Pierre Michaud was a member of the program committee of the Third Data Prefetching Championship (DPC3)
- Isabelle Puaut was a member of the program committee of the Euromicro Conference on Real Time Systems (ECRTS) 2019 and 2020, IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) 2020, Real Time Systems Symposium (RTSS) in 2019.
- 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 International Conference on Real-Time Networks and Systems (RTNS) 2019 and 2020.
- Isabelle Puaut was a member of the program committee of the 18th Workshop on Worst-Case Execution Time Analysis (WCET 2019).
- Erven Rohou and Caroline Collange were members of the program committee of the French *Conférence francophone en informatique autour des thématiques du parallélisme, de l'architecture et des systèmes* (Compas 2019).
- Erven Rohou was a member of the program committee of the Special Session on Compiler Architecture, Design and Optimization (CADO) of HPCS 2019.
- André Seznec was a member of program committee of ACM/IEEE Micro 2019 conference
- André Seznec is a member of program committee of ACM/IEEE ISCA 2020 conference
- André Seznec is a member of program committee of the IPDPS 2020 conference

*10.1.1.2. Reviewer*

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

### 10.1.2. Journal

*10.1.2.1. 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 ACM Transactions on Architecture and Compiler Optimization.

*10.1.2.2. Reviewer - Reviewing Activities*

Members of PACAP routinely review submissions to numerous international journals.

### 10.1.3. Invited Talks

Erven Rohou and Byron Hawkins gave invited talks at the 13th *rencontres de la communauté française de compilation*.

Erven Rohou gave an invited talk at the GDR SOC2 day in Nantes.

Erven Rohou gave a talk at the Compas 2019 conference.

André Seznec was an invited speaker at the RISC V workshop in Paris.

### 10.1.4. Leadership within the Scientific Community

Caroline Collange is a member of the steering committee of the *Conférence francophone en informatique autour des thématiques du parallélisme, de l'architecture et des systèmes* (Compas 2019).

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).

### 10.1.5. Research Administration

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).

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").

Erven Rohou is a member of the steering committee of the high security research laboratory (LHS).

Erven Rohou is a member of the "Comité de Centre" of the Inria Rennes Research Center.

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

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

- Licence: Nicolas Bellec, Système, 14 hours, L3, Université de Rennes 1, France
- License: Nicolas Bellec, Informatique, 14 hours, L1, Lycée Chateaubriand (Rennes), France
- Arthur Blanleuil, SYS1 (Systèmes mono-utilisateur), 18 hours, M1, Université Rennes 1, France
- Arthur Blanleuil, NOY (Systèmes d'exploitation – implémentation de noyaux de systèmes), 22 hours, M1, Université Rennes 1, France
- Arthur Blanleuil, SE (Système d'Exploitation), 24 hours, M1, Université Rennes 1, France
- Master: C. Collange, GPU programming, 20 hours, M1, Université de Rennes 1, France
- Licence: D. Hardy, Real-time systems, 68 hours, L3, Université de Rennes 1, France
- Master: D. Hardy, Operating systems, 59 hours, M1, Université de Rennes 1, France
- Master: Kévin Le Bon, Architecture à Objet Canonique, 20 hours, M2, Université de Rennes 1, France
- Licence: Kévin Le Bon, SI2, 40, L1, Université de Rennes 1, France
- Master: I. Puaut, Operating systems: concepts and system programming under Linux (SEL), 77 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Operating systems kernels (NOY), 54 hours, M1, Université de Rennes 1, France
- Master: I. Puaut, Real-time systems, 40 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.

### 10.2.2. Supervision

PhD: Arif Ali Ana-Pparakkal, *Performance Centric Dynamic Function Level Binary Transformation* [15], Université de Rennes 1, 9 Dec 2019, advisor E. Rohou

PhD in progress : Nicolas Bellec, *Security in real-time embedded systems*, started Dec 2019, advisors I. Puaut (50 %), G. Hiet from CIDRE (25 %), F. Tronel from CIDRE (25 %)

PhD in progress: Arthur Blanleuil, *Thread convergence prediction for SIMT architectures*, Université de Rennes 1, started Oct 2018, advisor C. Collange and A. Seznec

PhD in progress: Niloofar Charmchi, *Hardware prefetching and related issue*, Université de Rennes 1, started Jan 2017, advisors A. Seznec and C. Collange

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

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

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

### 10.2.3. Juries

Isabelle Puaut was a member of the following PhD thesis and habilitation thesis committees:

- Muhammad Refaat Sedky Soliman (PhD thesis), *Automated Compilation Framework for Scratchpad-based Real-Time Systems*, University of Waterloo, Canada, Juin 2019 (reviewer)
- Amine Naji (PhD thesis), *Timing Analysis for Time-Predictable Architectures*, Sorbonne Université, June 2019 (reviewer)
- Luca Santinelli (habilitation), *Mixed Criticality Modeling and Analysis Paradigms for Real Time Embedded Systems*, Habilitation à diriger des recherches, Institut National Polytechnique de Toulouse, May 2019 (reviewer)
- Roberto Medina (PhD thesis), *Deployment of Mixed-Criticality and Data-Driven Systems on Multi-core Architectures*, Université de Paris Saclay, January 2019

Isabelle Puaut was a member of the following hiring committees of assistant professors/professors:

- Professor, Université de Bretagne Occidentale, "methods and tools for the design of embedded systems, Systems on Chips, embedded systems and architectures"
- Professor, ENS Lyon
- Assistant professor, Université de Strasbourg, "performance, modeling and simulation"
- Assistant professor, ISAE-ENSMA Poitiers, "embedded real-time systems, data and model engineering"

Erven Rohou was a member of the following hiring committee (comités de sélection):

- Assistant professor position at Université de Grenoble on cloud and edge computing

Erven Rohou was a member of the following PhD thesis committees:

- Julien Proy, *Sécurisation systématique d'applications embarquées contre les attaques physiques*, June 2019 (reviewer).
- Nicolas Belleville, *Compilation pour l'application de contre-mesures contre les attaques par canal auxiliaire*, Université Grenoble Alpes, Nov 2019 (reviewer).
- Patryk Kiepas, *Performance analyses and code transformations for MATLAB applications*, Dec 2019 (reviewer).
- Paul Godard, *Parallélisation et passage à l'échelle durable d'une chaîne de traitement graphique pour l'impression professionnelle*, Université de Strasbourg, Dec 2019 (reviewer).

## 10.3. Popularization

### 10.3.1. Internal or external Inria responsibilities

Caroline Collange is a member of the committee of the Gilles Kahn PhD prize of Société Informatique de France.

### 10.3.2. Articles and contents

- Erven Rohou gave an interview in the *Émergences* magazine on (volume 56, Mar 22nd 2019) on automatically masking sensitive information to protect against side-channel attacks.

### 10.3.3. Education

Nicolas Bellec and Isabelle Puaut taught *Basics of computer architecture*, a training of high school teachers as part of the opening of the new computer science option in the two final years before Baccalauréat, 10 hours.

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

Erven Rohou was present at the International Cybersecurity Forum in Lille (FIC https://www.forum-fic.com/en/home.htm). He presented a demo on compiler-generated countermeasures against side-channel attacks, developed within the context of the CHIST-ERA SECODE project.

### 10.3.5. Internal action

Erven Rohou presented the activities of PACAP at the SecDays event organized at Inria Rennes and IRISA.

<p style="text-align: center; color: red;">**HYCOMES Project-Team**</p>

# 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 Program Committee of the Modelica Conference 2019.
- Khalil Ghorbal has served on the Program Committee of the VMCAI 2019 conference.
- Benoît Caillaud has served on the Steering Committee of the ACSD 2019 conference.

### 9.1.2. Invited Talks

Albert Benveniste has given an invited talk titled "Why considering nonstandard semantics for hybrid systems and how to reconcile it with superdense time semantics" at the Oded Maler Memorial workshop at the HSCC'19 conference in Montreal, Canada.

### 9.1.3. Leadership within the Scientific Community

Albert Benveniste is member of the French Académie des Technologies.

### 9.1.4. Scientific Expertise

- In 2019, Benoît Caillaud has reviewed collaborative research project proposals submitted to the French national funding agency ANR. As an Inria Evaluation Committee member, he has served on several Inria hiring and promotion committees.
- Albert Benveniste is president of the Scientific Council of Orange and member of the Scientific Council of Safran.

### 9.1.5. 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.

## 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

---

[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

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.

PhD: Joan Thibault, Structural Analysis Techniques for Binary Decision Diagrams, university of Rennes 1, co-supervised by Benoît Caillaud and Khalil Ghorbal.

### 9.2.3. *Juries*

Benoît Caillaud has served as president of the jury for Hugo Bazille's PhD defense, at the University of Rennes 1.

## 9.3. Popularization

### 9.3.1. *Internal action*

The Hycomes team has hosted short internships for secondary school students. This has been an opportunity to promote women in computing, since three female students visited the team for four days, to discover what scientific research is, and what research in computer science could mean. All team members contributed to the initiative.

---

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

<span style="color:red">**Kairos Project-Team**</span>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

- F. Mallet was Track Scientific Chair for DATE2019 organized in Firenze in March 2019.
- E. Madelaine is Chair of the Steering Committee of the Formal Aspects of Component Systems (FACS) conference.
- J.Deantoni was Chair of the first international workshops on "Multi-Paradigm Modeling for Cyber-Physical Systems" and "Modeling Language Engineering and Execution".
- J.Deantoni was Chair of "Computational Science" track of the RIVF 2019 conference.

### 10.1.2. Scientific Events: Selection

*10.1.2.1. Chair of Conference Program Committees*

- F. Mallet was Program Co-Chair of the 10th Workshop on Formal Techniques for Safety Critical Systems (FTSCS), organized as a satellite event of ICFEM 2019, in Shenzhen, Chine, in November 2019.
- F. Mallet was Program Co-Chair of ICTERI 2019 organized in Kherson, Ukraine, in May 2019.

*10.1.2.2. Member of the Conference Program Committees*

- J.Deantoni was in the program committee of: CoSim-CPS'19 and DSD'19
- F. Mallet was in the program committees of SEFM'19, DATE'19, FDL'19, DSD'19, Modelsward'19.
- D. Potop-Butucaru was in the program committee of FDL'19 and ACSD'19

*10.1.2.3. Reviewer*

- E. Madelaine is reviewer for the Formal Aspects of Component Systems (FACS), and industrial Formal Methods (iFM) conferences.
- L. Liquori and Claude Stolze reviewed for the conference FOSSACS/ETAPS.

### 10.1.3. Journal

*10.1.3.1. Member of the Editorial Boards*

- F. Mallet is now in the editorial board of Springer journal Software-Intensive Cyber-Physical Systems (SICS) dedicated to all topics around software in embedded and cyber-physical systems.
- F. Mallet was guest editor for a special issue of Elsevier Science of Computer Programming dedicated to the Theoretical Aspects of Software Engineering.

*10.1.3.2. Reviewer - Reviewing Activities*

- E. Madelaine was reviewer for the Journal of Systems and Software (JSS), and for Science of Computer Programming (SCP).
- L. Liquori and Claude Stolze reviewed for Fundamenta Informaticae.
- F. Mallet was reviewer for IEEE Transactions on Software Engineering (TSE) and Elsevier Journal on Microprocessors and Microsystems (MICPRO).

### 10.1.4. Invited Talks

- J.Deantoni was invited for a talk in the Danang University during the RIVF conference.
- J.Deantoni was invited for a talk during the "Computer Automated Multi-Paradigm Modelling 2019" meeting in Bellairs.
- F. Mallet was invited as a keynote speaker to the 11th IEEE TASE 2019 organized in Guilin, Chine (July 2019).
- L. Liquori is invited for a talk at the Bamberg University, Jan 2020.

### 10.1.5. Scientific Expertise

- F. Mallet is an elected member of the Conseil National des Universités (CNU) for section 27.
- F. Mallet has made an expertise of projects for the Belgium Agency of Research (FNRS).

### 10.1.6. Research Administration

- F. Mallet is Deputy Director of UMR I3S Laboratory and as such, member of its "comité de direction" and "conseil de laboratoire", together with the 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. She has been recently appointed member of UCA Academic Council.
- Luigi Liquori is member of the IFIP working group WG1.6 on Rewriting.

## 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.

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

Master:Marie-Agnès Paraldi Frati, Web Security and IoT Platform, 20h eq TD, Master 2 SICOM, Univ Avignon.

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

Master: Luigi Liquori, Rewriting Systems and Pattern Matching, 12 eq TD, Université de Lorraine.

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

Ph.D.: 12th International School on Rewriting (ISR) July 2020, Spain. Luigi Liquori. Pattern matching $\lambda$-calculi.

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, 32h eq TD, Polytech'Nice.

Master: Julien Deantoni, Language Interpreter, 32h eq TD, Polytech'Nice.

Master: Julien Deantoni, Micro-controller programming, 8h eq TD, Polytech'Nice.

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

Master: Dumitru Potop-Butucaru, Real-time embedded systems, 42h, EIDD (École d'Ingenieur Denis Diderot), Paris

### 10.2.2. Supervision

- HDR : Julien Deantoni, *Towards Formal System Modeling: Making Explicit and Formal the Concurrent and Timed Operational Semantics to Better Understand Heterogeneous Models*, Université Côte d'Azur, Juillet 2019 [13]
- PhD : Claude Stolze, Combining union, intersection and dependent types in an explicitly typed lambda-calculus, Université Côte d'Azur, Dec 16th 2019, Luigi Liquori. [14]
- PhD in progress : Carsten BRUNS, Performance analysis and optimisation of C++ applications, Université Côte d'Azur, 2021, Sid TOUATI.
- PhD in progress : Giovanni Liboni, Coordination of discrete (Cyber) Models, Université Cote d'Azur, end 2021, Frédéric Mallet, Julien DeAntoni.
- PhD in progress : Joelle Abou Faysal, A Formal Language for Ensuring Safety Scenarios in Autonomous Vehicles, Université Cote d'Azur, 2022, Frédéric Mallet.
- PhD: Keryan Didier, Contributions to the safe and efficient parallelisation of hard real-time systems. Sorbonne University, September 19, 2019, Dumitru Potop-Butucaru.
- PhD in progress : Hugo Pompougnac, Sorbonne University, 2022, Dumitru Potop-Butucaru.

### 10.2.3. Juries

- Frederic Mallet was president of the PhD Jury of Ines Array, Université Cote d'Azur, March 2019.
- Eric Madelaine was member of the PhD jury of Frédéric Lemoine (CNAM, Paris), July 2019.
- Frederic Mallet was reviewer for the PhD Jury of Frédéric Giroudot (ISAE, Toulouse), December 13th 2019.
- Frederic Mallet was reviewer for the PhD Jury of Ngo Minh Thang NGUYEN (Centrale Supélec/CEA), December 16th 2019.
- Dumitru Potop-Butucaru was a member of the PhD jury of Lina Marsso (Univ. Grenoble-Alpes, Inria, CNRS, GrenobleINP), December 10, 2019.
- Dumitru Potop-Butucaru was a member of the PhD jury of Pierre Donat-Bouilloud (Sorbonne University), December 6, 2019.
- Luigi Liquori was member of the PhD jury of Claude Stolze, Université Côte d'Azur, December 2019.

## 10.3. Popularization

### 10.3.1. Interventions

Luigi Liquori. Table ronde: "Journée Internationale du m-Tourisme 2019. Blockchain for Tourism", M-Tourism Day, Telecom Valley, Panel, Cannes, 2019.

<span style="color:red">**KOPERNIC Team**</span>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. Local Chair*

The Kopernic team has hosted the 10th edition of the RTSOPS in July 2019.

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Chair of Conference Program Committees*

Liliana Cucu-Grosjean is the track chair of IEEE RTSS2019 and DATE2020 Track co-chair for real-time systems

*9.1.2.2. Member of the Conference Program Committees*

- Liliana Cucu: ACM RACS, RTNS, WFCS

### 9.1.3. Journal

*9.1.3.1. 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, etc.

### 9.1.4. 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).

### 9.1.5. Research Administration

- Liliana Cucu-Grosjean is co-chair of Inria Committee on gender equality and equal opportunities
- Yves Sorel is chair of the CUMI Paris center commission
- Liliana Cucu-Grosjean was member of Inria Evaluation Commission until September 2019
- Liliana Cucu-Grosjean is member of Inria Scientific Board and CAP CRCN since September 2019
- Liliana Cucu-Grosjean is member of Paris CLHSCT
- Liliana Cucu-Grosjean is member of CES Paris commission
- Yves Sorel is member of the CDT Paris center commission

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

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

Engineering school: Liliana Cucu-Grosjean, Graph theory, 30H, ESIEE, Cergy, France

Master: Liliana Cucu-Grosjean, Software Engineering, 30H, ESIEE, Noisy-le-Grand, France

Master: Adriana Gogonel, Machine learning, 30H, ESIEE, Noisy-le-Grand, France

### *9.2.2. Supervision*

PhD in progress: Kevin Zagalo, Statistical predictability of cyber-physical systems, UMPC, started on October 2019, supervised by Liliana Cucu and Prof. Avner Bar-Hen (CNAM)

PhD in progress: Evariste Ntaryamira, Analysis of embedded systems with time and security constraints, UPMC, started on May 2017, supervised by Liliana Cucu and Cristian Maxim (IRT SystemX)

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

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

### *9.2.3. Juries*

- Yves Sorel was a HDR jury member for the thesis of Luca Santinelli (ONERA), defended in May 2019.
- Liliana Cucu-Grosjean was a Phd reviewer for the thesis of Roberto Medina (Telecom Paristech), defended in January 2019.
- Liliana Cucu-grosjean was a PhD jury member of Francesco Pozo (Malardelan, Sweden), defended in October 2019.

## 9.3. Popularization

### *9.3.1. Articles and contents*

- Interview with the Statinf co-founders, published on Inria web site (https://www.inria.fr/centre/paris/actualites/statinf-sonde-les-caeurs-des-systemes-embarques)

### *9.3.2. Education*

- Presentation of Adriana Gogonel at a day organized by a Creteil and Versailles Academy for outreaching Computer Science (April 2019, Paris)

### *9.3.3. Interventions*

- Participation of Adriana Gogonel at a round table entitled "May we innovate within a research institute?" (March 2019, Rocquencourt).

<p align="center" style="color:red"><b>PARKAS Project-Team</b></p>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Selection

*9.1.1.1. Chair of Conference Program Committees*

- T. Bourke co-chaired the program committee of the ACM/IEEE international conference on Embedded Software (EMSOFT 2019).

*9.1.1.2. Member of the Conference Program Committees*

- T. Bourke served on the PC of the Euromicro Conference on Real-Time Systems (ECRTS 2019).
- T. Bourke served on the PC of the international workshop on Software and Compilers for Embedded Systems (SCOPES 2019).
- T. Bourke served on the PC of the international Modelica conference (MODELICA 2019).
- T. Bourke served on the PC of the OCaml Users and Developers Meeting (OCaml 2019).
- M. Pouzet served on the PC of the program committee of the ACM/IEEE international conference on Embedded Software (EMSOFT 2019).
- M. Pouzet served on the PC of the international workshop on Software and Compilers for Embedded Systems (SCOPES 2019).
- M. Pouzet served on the PC of the international workshop on Cyber-Physical Systems (CyPhy), a satellite event of ESWEEK.
- F. Zappa Nardelli served on the PC of the international conference on Object-Oriented Programming, Systems, Languages & Applications (OOPSLA 2019).
- F. Zappa Nardelli served on the PC of the ACM Workshop on Gradual Types (WGC 2020).

*9.1.1.3. Reviewer*

- T. Bourke reviewed submissions for the international conference on Computer Aided Verification (CAV 2019)
- T. Bourke reviewed submisssions for the international conference on Object-Oriented Programming, Systems, Languages & Applications (OOPSLA 2019).

### 9.1.2. Journal

*9.1.2.1. Reviewer - Reviewing Activities*

- T. Bourke reviewed articles for the Journal of Logical and Algebraic Methods in Programming (JLAMP).

### 9.1.3. Research Administration

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

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

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

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

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

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

Master: M. Pouzet: "Synchronous Reactive Languages" (M2), Lectures, Master COMASIC (École Polytechnique) and FIL (Université Paris-Sud, Saclay), France

Master: T. Bourke, lab classes for "A Programmer's introduction to Computer Architectures and Operating Systems" (M1), École Polytechnique, France

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

Bachelor: F. Zappa Nardelli: "A Programmer's introduction to Computer Architectures and Operating Systems", 20h, École Polytechnique, France

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

M1 Projects: T. Bourke is directing two M1 research projects.

### 9.2.2. Supervision

- PhD in progress: Lélio Brun, under review, supervised by T. Bourke and M. Pouzet.
- PhD in progress: Ismail Lakhim-Bennani, 1st year, supervised by M. Pouzet, G. Frehse, and T. Bourke
- PhD in progress: Basile Clément, 1st year, supervised by F. Zappa Nardelli and M. Pouzet.
- PhD: Chandan Reddy, supervised by A. Cohen, defended in March 2019.
- PhD: Ulysse Beaugnon, supervised by A. Cohen and M. Pouzet, defended in June 2019.

### 9.2.3. Juries

- T. Bourke was a jury member for the for the PhD thesis of Steven Varoumas, November 2019.
- F. Zappa Nardelli was a jury member for the PhD thesis of Francois Ginraud, Grenoble, Jan 2019.

## 9.3. Popularization

### 9.3.1. Internal or external Inria responsibilities

- T. Bourke participated in the *commission d'emplois scientifiques* (postdocs, delegations, and PhDs) for the Inria Paris research centre.
- T. Bourke participated in the PhD progress committees (*suivi doctorale*) for B. Medeiros de Barros and N. Kulatova.
- T. Bourke and M. Pouzet participated in meetings with the *Ministère de la Transition écologique et solidaire* on the validation of autonomous driving systems.

<p style="text-align:center; color:red;">**SPADES Project-Team**</p>

# 9. Dissemination

## 9.1. Environmental and societal responsibility

NB: We support the idea of an additional section in future Activity Reports that would be dedicated to actions in connection with our environmental and societal responsibility. We write below content that would fit into it for 2019.

- A discussion on computer ethics was scheduled at our last team seminar. There have been several meetings between permanent researchers to discuss how we can better align our research agenda with the current needs of our society. Our discussions cover aspects such as the environmental and societal impact of ICT (Information and Communication Technologies), and more broadly the role that ICT play in our lives, our role as researchers in computer science, etc. These discussions have led us to consider these issues as a research topic that we should investigate in the near future.

- Sophie Quinton and Jean-Bernard Stefani contributed to the so-called "MakeSEnS" working group appointed by the CEO of Inria to propose a list of concrete actions that the institute could take to tackle the current environmental crisis [24].

- Sophie Quinton has been mandated by Patrick Gros (Director of the Inria Grenoble – Rhône-Alpes research center) to organize discussions and actions regarding the environmental and societal impact of our research at Inria Grenoble Rhône-Alpes.

- Sophie Quinton is a member of the GDS EcoInfo (https://ecoinfo.cnrs.fr/). Her actions as member of EcoInfo include: leading a discussion group on the environmental impact of collaborative platforms as part of a two-day seminar organized at Mines ParisTech [0]; and contributing to a roadmap regarding the environmental and societal impact of ICT prepared by the Conseil National du Numérique (https://cnnumerique.fr/) at the government's request.

- Sophie Quinton co-chairs a working group of the GDR CIS associated with the Center for Internet and Society (http://cis.cnrs.fr/) focused on environmental issues.

- Sophie Quinton is part of the scientific committee of the upcoming "COP2 étudiante" (https://cop2etudiante.org/).

## 9.2. Promoting Scientific Activities

### 9.2.1. Scientific Events: Organisation

#### 9.2.1.1. 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.

#### 9.2.1.2. Member of the Organizing Committees

- Alain Girault was co-organizer of the Workshop on Synchronous Programming (SYNCHRON'19) http://synchron19.org.

---

[0]http://www.mines-paristech.fr/Actualites/Ingenieurs-et-transitions-environnementales/4116

- Gregor Gössler was co-organizer of a Shonan seminar on *Causal reasoning in systems* https://project. inria.fr/shonan139.

### 9.2.2. Scientific Events: Selection

*9.2.2.1. Chair of Conference Program Committees*

- Sophie Quinton was the program chair of 31st Euromicro Conference on Real-Time Systems (ECRTS'19) https://www.ecrts.org/archives/fileadmin/WebsitesArchiv/ecrts2019/index.html.

*9.2.2.2. Member of the Conference Program Committees*

- Alain Girault served in the program committees of the Forum on specification and Design Languages (FDL'19) and the Conference on Applications of Concurrency to System Design (ACSD'19).
- Gregor Gössler served in the program committees of the ACM/IEEE International Conference on Embedded Software (EMSOFT'19), the 26th SPIN Symposium on Model Checking of Software (SPIN'19), the 17th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE'19), and the 4th international Workshop on Formal Reasoning about Causation, Responsibility, and Explanations in Science and Technology (CREST'19).

*9.2.2.3. Reviewer*

- Alain Girault reviewed an article for the International Conference on Fundamental Approaches to Software Engineering (FASE'19).
- Sophie Quinton reviewed an article for the ACM International Conference on Embedded Software (EMSOFT'19).
- Pascal Fradet reviewed an article for the ACM International Conference on Embedded Software (EMSOFT'19).

### 9.2.3. Journal

*9.2.3.1. Member of the Editorial Boards*

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

*9.2.3.2. Reviewer - Reviewing Activities*

- Alain Girault reviewed articles for IEEE Transactions on Service Computing (TSC) and for the International Journal on Software Tools for Technology Transfer (STTT).
- Gregor Gössler reviewed an article for IEEE Transactions on Automatic Control (TAC).

### 9.2.4. Leadership within the Scientific Community

- Sophie Quinton is a member of the ACM SIGBED Executive Committee and Associate Editor of the SIGBED Review.

### 9.2.5. Research Administration

- Pascal Fradet is head of the committee for doctoral studies ("Responsable du comité des études doctorales") of the Inria Grenoble – Rhône-Alpes research center and local correspondent for the young researchers Inria mission ("Mission jeunes chercheurs").
- Alain Girault is Deputy Scientific Director at Inria in charge of the domain "Algorithmics, Programming, Software and Architecture". He is also Scientific Manager of the Cyber-Physical Systems axis of the Persyval-Lab labex https://persyval-lab.org.
- 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.

# 9.3. Teaching - Supervision - Juries

### 9.3.1. Teaching

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

Licence : Pascal Fradet, Modèles de Calcul : $\lambda$-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, Analyse de Code pour la Sûreté et la Sécurité, 45 HeqTD, niveau M1, Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Théorie des Langages 1, 48 HeqTD, niveau L3. Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Théorie des Langages 2, 37,5 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Xavier Nicollin, Bases de la Programmation Impérative, 30 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Licence : Sophie Quinton, Théorie des Langages 2, 20 HeqTD, niveau L3, Grenoble INP (Ensimag), France

Master : Sophie Quinton, Performance and Quantitative Properties, 8 HeqTD, MOSIG, Univ. Grenoble Alpes, France

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

### 9.3.2. 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: Thomas Mari, "Construction of Safe Explainable Cyber-physical systems"; Grenoble INP; since October 2019; co-advised by Gregor Gössler and Thao Dang.

- PhD: Christophe Prévot, "Early Performance assessment for evolving and variable Cyber-Physical Systems", Univ. Grenoble Alpes; defended on November 15th, 2019; co-advised by Alain Girault and Sophie Quinton.

- PhD: Zain A. H. Hammadeh, "Deadline Miss Models for Temporarily Overloaded Systems", TU Braunschweig; defended on May 28th, 2019; co-advised by Rolf Ernst 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, "RDF: A reconfigurable dataflow MoC supporting dynamic topological transformations and static analyzability"; 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.

- Internships: Jonathan Julou and Martin Portalier, "Formal proofs for real-time systems analysis"; ENSIMAG; co-advised by Pascal Fradet, Xiaojie Guo, Maxime Lesourd and Sophie Quinton.

### 9.3.3. Juries

- Alain Girault was referee for the Habilitation thesis of Julien De Antoni (Université Côte d'Azur) and was member of the PhD thesis of Pierre Donat-Bouillud (Sorbonne Université). He was also vice-president of the Inria Starting Research Position (SRP) Advanced Research Position (ARP) jurys.
- Jean-Bernard Stefani was examiner for the Habilitation (HDR) jury of Thomas Ledoux (Université de Nantes).
- Sophie Quinton was a member of the PhD thesis committee of Hugo Daigmorte (Université de Toulouse).

## 9.4. Popularization

### 9.4.1. Articles and contents

Software is a fundamental pillar of modern scientific research, across all fields and disciplines. However, there is a lack of adequate means to cite and reference software due to the complexity of the problem in terms of authorship, roles and credits. This complexity is further increased when it is considered over the lifetime of a software that can span up to several decades. Building upon the internal experience of Inria, we have provided a contribution to the ongoing efforts in order to develop proper guidelines and recommendations for software citation and reference. Namely, we recommend: (1) a richer taxonomy for software contributions with a qualitative scale; (2) to put humans at the heart of the evaluation; and (3) to distinguish citation from reference [10]. This has been a joint work between Alain Girault and colleagues from Software Heritage (Roberto Di Cosmo), from Inria's Evaluation Committee (Pierre Alliez, Benjamin Guedj, Mohand-Saïd Hacid, Nicolas Rougier), and a specialist in reproducible research (Arnaud Legrand).

### 9.4.2. Interventions

Sophie Quinton played the role of one of the experts in the fictional trial of a robot during the Transfo Festival in Grenoble. She also gave a lecture on the design and verification of real-time systems as part of the ISN curriculum for high school teachers.

Alain Girault played the role of one of the experts in the fictional trial of a robot during the Fête de la Science in Grenoble.

### 9.4.3. Creation of media or tools for science outreach

All SPADES members have contributed to the scenario of an animated movie, commissioned by the communication service of Inria, in order to popularise the research activities of SPADES.

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events Selection

Jean-Pierre Talpin served in the program committee of the ACM LCTES'19, ACM SAC'19 and SCOPES'19 conferences.

Thierry Gautier reviewed articles for *Journal of Systems Architecture* (Elsevier).

### 10.1.2. Journal

Jean-Pierre Talpin is Associate Editor with the ACM Transactions for Embedded Computing Systems (TECS).

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

### 10.1.3. Invited Talks

Jean-Pierre Talpin gave an invited presentation entitled "Towards verified programming of embedded devices" at DATE'19, Florence.

## 10.2. Teaching - Supervision - Juries

Jean-Pierre Talpin gave a one week graduate-level course at the Sheng Yuan Honors College, BUAA, entitled: "introduction to program verification".

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

Thierry Gautier served as external assessor for professor position application at Nankai University (China).

<p style="text-align:center; color:red; font-weight:bold;">ANTIQUE Project-Team</p>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. 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 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).
- Caterina Urban is a member of the Executive Board of ETAPS (European Joint Conferences on Theory & Practice of Software).

*10.1.1.2. Member of the Organizing Committees*

Caterina Urban serves as Chair of the Award Committee of the ETAPS Doctoral Dissertation Award 2020.

### 10.1.2. Event organization

- Cezara Drăgoi co-organize "VDS: Workshop on Verification of Distributed Systems" https://goto.ucsd.edu/vds/ with Klaus v. Gleissenthall from Univerisity of California, San Diego. This is a workshop that brings together two communities: verification and distributed systems by having participants from the two communities.

### 10.1.3. Scientific Events: Selection

*10.1.3.1. Member of the Conference Program Committees*

- Jérôme Feret served as a Member of the Program Committee of SASB 2019 (Static Analysis and Systems Biology).
- Jérôme Feret served as a Member of the Program Committee of CMSB 2019 (Computational Methods in Systems Biology).
- Jérôme Feret served as a Member of the Program Committee of CIBCB 2019 (Computational Intelligence in Bioinformatics and Computational Biology).
- Jérôme Feret served as a Member of the Program Committee of HSB 2019 (Hybrid Systems Biology).
- Jérôme Feret is serving as a member of the Program Committee of CMSB 2020 (Computational Methods in Systems Biology).
- Jérôme Feret is serving as a member of the Program Committee of HSB 2020 (Hybrid Systems Biology).
- Xavier Rival served as a Member of the Program Committee of SAS 2019 (Static Analysis Symposium).
- Xavier Rival is serving as a Member of the Program Committee of POPL 2020 (Symposium on Principles Of Programming Languages).
- Caterina Urban served as a member of the Program Committee of VMCAI 2019 (Verification, Model Checking, and Abstract Interpretation).

- Caterina Urban served as a member of the Artifact Evaluation Committee of POPL 2019 (Symposium on Principles of Programming Languages).
- Caterina Urban served as a member of the Program Committee of CAV 2019 (Computer Aided Verification).
- Caterina Urban served as a member of the Artifact Evaluation Committee of PLDI 2019 (Programming Languages Design and Implementation).
- Caterina Urban served as a member of the Program Committee of NSV 2019 (International Workshop on Numerical Software Verification).
- Caterina Urban served as a member of the Program Committee of LOPSTR 2019 (Logic-based Program Synthesis and Transformation).
- Caterina Urban served as a member of the Program Committee of TAPAS 2019 (Workshop on Tools for Automatic Program Analysis).
- Caterina Urban served as a member of the Program Committee of EMSOFT 2019 (Embedded Software).
- Caterina Urban served as a member of the Program Committee of iFM 2019 (integrated Formal Methods).
- Caterina Urban serves as a member of the Program Committee of VMCAI 2020 (Verification, Model Checking, and Abstract Interpretation).
- Caterina Urban serves as a member of the Program Committee of ESOP 2020 (European Symposium on Programming).
- Caterina Urban serves as a member of the Program Committee of CAV 2020 (Computer Aided Verification).
- Caterina Urban serves as a member of the Program Committee of SOAP 2020 (Workshop on the State Of the Art in Program Analysis).
- Cezara Drăgoi served as a member of the Program Committee of POPL 2020 (Symposium on Principles of Programming Languages)
- Cezara Drăgoi served as a member of the Program Committee of PLDI 2020 (Symposium on Programming Languages Design and Implementations)
- Cezara Drăgoi served as a member of the Program Committee of CAV 2019 (Computer Aided Verification).
- 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 2019 (Conference on Networked Systems).

*10.1.3.2. Reviewer*

- Marc Chevalier served as Reviewer for SAS 2019 (Static Analysis Symposium).
- Marc Chevalier served as Reviewer for VMCAI 2020 (Verification, Model Checking, and Abstract Interpretation).
- Jérôme feret served as Reviewer for CAV 2019 (computer aided verification).
- Xavier Rival served as Reviewer for ESOP 2020 (European Symposium on Programming).
- Caterina Urban served as Reviewer for NFM 2019 (NASA Formal Methods).
- Caterina Urban served as Reviewer for POPL 2020 (Symposium on Principles of Programming Languages).

## 10.1.4. Journal

*10.1.4.1. 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 served as co-Editor of an Issue of the Theoretical Computer Science journal, that is composed of papers from SASB 2016 and VEMP 2016, and appeared in 2019.
- Jérôme Feret served 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 appeared in 2019.

*10.1.4.2. Reviewer - Reviewing Activities*

- Jérôme Feret served as a Reviewer for Fundamenta Informaticæ.
- Jérôme Feret served as a Reviewer for Theoretical Computer Science.
- Jérôme Feret served as a Reviewer for Transactions on Computational Biology and Bioinformatics.

### 10.1.5. Invited Talks

- Caterina Urban was invited to give a talk at the Gran Sasso Science Institute, L'Aquila, Italy.
- Caterina Urban was invited to give a talk at SAS 2019 (Static Analysis Symposium) [13].

### 10.1.6. Leadership within the Scientific Community

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

### 10.1.7. Scientific Expertise

- Jérôme Feret reviewed 5 proposals for the Prin 2017 (Research Projects of National Relevance) Program (Italian Ministry of Education and Research)

### 10.1.8. Research Administration

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

## 10.2. Teaching - Supervision - Juries

### 10.2.1. 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, "Functional Programming", 21h, L3, Bachelor Programme at at École Polytechnique, France.

Master:

- Xavier Rival, "Introduction to Static Analysis", 12h, Internet of Things Master (retraining curriculum, EXED), 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), Rule-based Modelling, 24h, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.

Doctorat:

- Jérôme Feret, "Abstract Interpretation of Models of Intracellular Signalling Pathways", 3h, CNRS summer school "Formal modeling of Biological Regulation Networks", June 2019, Île de Porquerolles, France.

### *10.2.2. Supervision*

- PhD defended: Andreea Beica, Abstraction of Biochemical Reaction Networks, started in 2015 and supervised by Vincent Danos
- PhD defended: Hugo Illous, Relational Shape Abstraction Based on Separation Logic, started in 2015 and supervised by Xavier Rival and Matthieu Lemerre (CEA)
- PhD in progress
- 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: Albin Salazar, Formal derivation of discrete models with separated time-scales, started in 2019 and supervised by Jérôme Feret
- PhD in progress: Olivier Nicole, Verification of micro-kernels, started in 2018 and supervised by Xavier Rival and Matthieu Lemerre (CEA)

### *10.2.3. Juries*

- Jérôme Feret served as a member for the Jury of the PhD of Andreea Beica (Defense on the 12th of June 2019)
- Xavier Rival served as a member for the Habilitation Thesis Committee of Chien Chung Huang (Defense on the 28th of January 2019)
- Xavier Rival is serving as a member of the Review Committee for Vincenzo Arceri at University of Verona (to be defended in early 2020).
- Caterina Urban served as a member of the Jury of the PhD of Emilio Incerto at the Gran Sasso Science Institute in Italy (defense on the 5th of April 2019).
- Cezara Drăgoi servered as a member for the Jury of the PhD of Hugo Illous, Relational Shape Abstraction Based on Separation Logic (defence on the 16th avril 2019 ).

## 10.3. Popularization

### *10.3.1. Internal or external Inria responsibilities*

- Cezara Drăgoi and Xavier Rival are elected members of the Inria Commision of Evaluation
- Jérôme Feret is a member of the jury of the SIF - Gilles Kahn PhD Award.
- 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.
- Cezara Drăgoi served in the jury for part-time positions at LiX, January 2019.
- Cezara Drăgoi served in the Inria jury for CES - delegations and Phd scholarships in 2019.

### *10.3.2. Articles and contents*

- Xavier Rival has been working with Kwangkeun Yi on the writing of a book that should serve as an introduction to the field of static analysis, for students and engineers, and this book is expected to be released by MIT Press in January 2020 [16].

### *10.3.3. Creation of media or tools for science outreach*

Xavier Rival has given a talk as part of the "Mon équipe en 180 secondes" series at Inria Paris.

<p style="text-align:center; color:red; font-weight:bold;">CAMBIUM Project-Team</p>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Selection

*9.1.1.1. Chair of Conference Program Committees*

François Pottier was the program chair of the International Conference on Functional Programming (ICFP 2019) which took place in Berlin, Germany in August 2019.

*9.1.1.2. Member of the Conference Program Committees*

Xavier Leroy was on the program committee of PERR 2019, the 3rd Workshop on Program Equivalence and Relational Reasoning, part of the ETAPS 2019 joint conferences.

Xavier Leroy was on the program committee of FOSSACS 2020, the 23rd International Conference on Foundations of Software Science and Computation Structures, part of the ETAPS 2020 joint conferences.

Didier Rémy was a member of the program committee for FLOPS 2020, the 15th International Symposium on Functional and Logic Programming.

### 9.1.2. Journal

*9.1.2.1. Member of the Editorial Boards*

Xavier Leroy is area editor for Journal of the ACM, in charge of the Programming Languages area. He is a member of the editorial board of Journal of Automated Reasoning.

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.

Until September 2019, Didier Rémy was a member of the ML Family workshop steering committee.

### 9.1.3. Scientific Expertise

Didier Rémy co-authored the Inria white book on Cybersecurity [17], [18] and a companion document of *Recommendations for Inria's Management*.

### 9.1.4. Research Administration

Damien Doligez chairs the Caml Consortium.

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 Inria's delegate in the MPRI's pedagogical and management board of the *Master Parisien de Recherche en Informatique* (MPRI).

Didier Rémy set up the Inria-Nomadic Labs partnership and is currently the co-chair of its steering committee.

# 9.2. Teaching - Supervision - Juries

## 9.2.1. Teaching

Master (M2): "Proofs of Programs", Jean-Marie Madiot, 18 HETD, MPRI, Université Paris Diderot, France.

Master (M2): "Programming shared memory multicore machines", Luc Maranget, 18 HETD, MPRI, Université Paris Diderot, France. Starting December 2019, Luc Maranget is in charge of this course.

Master (M2): "Functional programming and type systems", François Pottier, 18 HETD, MPRI, Université Paris Diderot, France.

Master (M2): "Functional programming and type systems", Didier Rémy, 18 HETD, MPRI, Université Paris Diderot, France. Didier Rémy is in charge of this course.

Licence (L3): Jean-Marie Madiot, "Introduction à l'informatique", 40 HETD, École Polytechnique, France.

Open lectures: Xavier Leroy, *Sémantiques mécanisées: quand la machine raisonne sur ses langages*, 19 HETD, Collège de France, France.

Summer school: Xavier Leroy, *Proving the correctness of a compiler*, 6 HETD, 2019 EUtypes summer school on Types for Programming and Verification, North Macedonia.

## 9.2.2. Supervision

PhD in progress: Frédéric Bour, "An interactive, modular proof environment for OCaml", Université Paris Diderot, since October 2019, advised by François Pottier and Thomas Gazagnaire (Taridès).

PhD in progress: Basile Clément, "Domain-specific language and machine learning compiler for the automatic synthesis of high-performance numerical libraries", École Normale Supérieure, since September 2018, advised by Xavier Leroy since October 2019.

PhD in progress: Nathanaël Courant, "Towards an efficient, formally-verified proof checker for Coq", Université Paris Diderot, since September 2019, advised by Xavier Leroy.

PhD: Armaël Guéneau, "Mechanized Verification of the Correctness and Asymptotic Complexity of Programs", Université Paris Diderot, defended on December 16, 2019 [11], advised by Arthur Charguéraud and François Pottier.

PhD in progress: Quentin Ladeveze, "Generic conditions for DRF-SC in axiomatic memory models", Université Paris Diderot, since October 2019, advised by Luc Maranget and Jean-Marie Madiot.

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: Thomas Williams, "Putting Ornaments into practice", Université Paris Diderot, since September 2014, advised by Didier Rémy.

## 9.2.3. Juries

Xavier Leroy participated in the hiring committee for a professor position at the UFR d'Informatique of U. Paris Diderot.

Xavier Leroy chaired the jury for the Habilitation defense of Yann Régis-Gianas (U. Paris Diderot, November 2019).

Xavier Leroy was external reviewer for the PhD of Andrea Condoluci (U. Bologna, to be defended in 2020).

Jean-Marie Madiot served as an examiner at the computer science oral examination for the "second concours" of École Normale Supérieure de Lyon.

Didier Rémy participated in the hiring committee for an Inria Centrale-Supélec Chair in cybersecurity.

# 9.3. Popularization

### 9.3.1. Interventions

Xavier Leroy was on the committee of the 2019 Sephora Berrebi scholarship for women in mathematics and computer science. At the award ceremony (Paris, France, February 2019), he gave a popular science talk on Grace Hopper and the birth of the compiler.

Xavier Leroy gave popularization talks on deductive software verification at the Aerospace Lab Conferences of ONERA (Palaiseau, France, June 2019) and at the Summer 2019 BOB conference (Berlin, Germany, August 2019).

<span style="color:red">**CELTIQUE Project-Team**</span>

# 6. Dissemination

## 6.1. Promoting Scientific Activities

### 6.1.1. Scientific Events: Organisation

*6.1.1.1. Member of the Conference Program Committees*

- Frédéric Besson: PriSC 2019 Workshop on Principles of Secure Compilation
- Sandrine Blazy: POPL 2020 (Symposium on Principles of Programming Languages), APLAS 2019 (Asian Symposium on Programming Languages and Systems), ITP 2019 (Conference on Interactive Theorem Proving), SpiSA 2019 (Workshop on Instruction Set Architecture Specification).
- Thomas Jensen: SAS 2019 (Static Analysis Symposium), ENTROPY 2019 (Enabling Trust through OS proofs).

*6.1.1.2. Reviewer*

- Frédéric Besson: TACAS

### 6.1.2. Journal

*6.1.2.1. Reviewer - Reviewing Activities*

- Frédéric Besson: Journal of Computer Security (JCS), Transactions on Software Engineering (TSE)
- Alan Schmitt: Theoretical Informatics and Applications (RAIRO ITA)

### 6.1.3. Invited Talks

- Frédéric Besson: GT Sécurité des Systèmes, des Logiciels et des Réseaux
- Sandrine Blazy: *The Verasco static analyzer*, Effective Verification: Static Analysis Meets Program Logics, Lorentz center, Netherlands, May. 2019
- Sandrine Blazy: *Formal Verification of a Constant-Time Preserving C Compiler*, Verified software workshop, Newton institute, Cambridge, United Kingdom, Sept. 2019
- Alan Schmitt: *Sémantiques Formelles et Certifiées*, 30 ans des JFLA
- Alan Schmitt: *Formal JavaScript*, Journées Nationales du GDR GPL
- Alan Schmitt: *Skeletal Semantics*, GT Langages, Types et Preuves

### 6.1.4. Leadership within the Scientific Community

- Sandrine Blazy is member of Section 6 of the national committee for scientific research CoNRS.
- Sandrine Blazy is member of IFIP WG 2.11 on program generation and of IFIP WG 1.9/2.15 on verified software.

### 6.1.5. Scientific Expertise

- Sandrine Blazy evaluated two Belgian FWO Grant research proposals.
- Sandrine Blazy is member of the Scientific Advisory Board of the Flemish Cybersecurity Initiative Flanders Program.
- Sandrine Blazy and David Pichardie were members of the HCERES evaluation committee of the LSV laboratory.
- Thomas Jensen was member of the HCERES evaluation committee of the University Grenoble–Alpes LIG laboratory.

- Thomas Jensen was vice-president of the ANR 2019 selection committee for research proposals in Computing and Communication (CES 25).

### 6.1.6. Research Administration

- Sandrine Blazy and Thomas Jensen are members of the steering committee of the international Static Analysis Symposium.

## 6.2. Teaching - Supervision - Juries

### 6.2.1. Teaching

License : Frédéric Besson, Functional programming, 28h, Insa3, Insa Rennes, France

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

Master : Sandrine Blazy, Semantics of Programming Languages, 20h, M1, Université Rennes 1, France

Master : Sandrine Blazy, Software vulnerabilities, 30h, M2, Université Rennes 1, 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 : Alan Schmitt, Programmation de Confiance, 30h, L3, Université Rennes 1, France

Licence : David Pichardie, Programmation, 30h, L3, ENS Rennes, France

Master : David Pichardie, Semantics of Programming Languages, 30h, M1, Université Rennes 1, France

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

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

Master : Thomas Genet, Enseigner l'informatique au lycée, 15h, M1, Université Rennes 1, France

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

Master : Benoît Montagu, Analyse et Conception Formelles, 16h, M1, Université Rennes 1, France

Master : Alan Schmitt, Suivi de Projet, 24h, M1, ENS Rennes, France

Master : Alan Schmitt, Advanced Semantics, 15h, M2, ENS Rennes, France

Master : Alan Schmitt, Preparation of Agregation exam, 20, M2, ENS Rennes, France

License : Thomas Jensen, Logic, 30h, Insa3, Insa Rennes, France

Master : Thomas Jensen, Software Security , 18h, M2, Université Rennes 1, France

### 6.2.2. Supervision

Phd : Alexandre Dang, Compilation for memory protection, Université Rennes 1, 10/12/2019, Thomas Jensen, Frédéric Besson

Phd : Julien Lepiller, Verifying Software Fault Isolation, Université Rennes 1, 11/12/2019, Thomas Jensen, Frédéric Besson

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

PhD in progress : Aurèle Barrière, Formal verification of a JIT compiler, September 2019, Sandrine Blazy and David Pichardie

PhD in progress : Samy Daoud, Modélisation formelle pour le déploiement et la reconfiguration automatique en ligne dans une infrastructure réseau et IT répartie, November 2018, Alan Schmitt

PhD in progress : Adam Khayam, Formal Semantics of Multitier Languages, July 2019, Alan Schmitt

PhD in progress : Guillaume Ambal, Sémantiques Squelettiques pour Calculs de Processus, September 2019, Alan Schmitt

PhD in progress : Louis Noizet, Compilation Certifiée de Sémantiques Squelettiques, October 2019, Alan Schmitt

Master 2 internship : Aurèle Barrière, Formal verification of a JIT compiler, February of June 2019, Sandrine Blazy and David Pichardie

Master 1 internship : Guillaume Barbier, Maxime Bridoux, Jean Jouve, Clément Legrand-Duchesne, Skeletal Semantics for WebAssembly, September 2018 to May 2019 Alan Schmitt

ENS 4th year internship : Nathanaël Courant, CFA Generation from a Skeletal Semantics, September 2019 to July 2019, Thomas Jensen and Alan Schmitt

ENS 4th year internship : Vincent Rebiscoul, Certified CFA Generation, September 2019 to February 2020, Thomas Jensen and Alan Schmitt

ENS 3th year internship : Justine Sauvage, Modèles formels pour la blockchain, May 2019 to July 2019, Thomas Genet and Thomas Jensen

## 6.2.3. *Juries*

- Sandrine Blazy, jury member for the selection of CNRS CR and DR (researchers) candidates, February and March 2019, CNRS, Paris, France.

- Sandrine Blazy, jury member (president) for the PhD defense of Simon Lunel, January 2019, Université Rennes 1

- Sandrine Blazy, jury member for the PhD defense of Joseph Lallemand, November 2019, Lorraine University, Nancy

- Sandrine Blazy, jury member for the HDR defense of Yann Régis-Gianas, November 2019, Paris University

- Sandrine Blazy, jury member (reviewer) for the PhD defense of Mathieu Journault, November 2019, Paris Sorbonne University

- Sandrine Blazy, jury member (president) for the PhD defense of Arif Ali Anapparakkal, December 2019, Université Rennes 1

- Sandrine Blazy, jury member (president) for the PhD defense of Julien Lepiller, December 2019, Université Rennes 1

- Sandrine Blazy, jury member of the GDR GPL PhD award committee

- Sandrine Blazy, member of hiring committee for a professor position, Spring 2019, UBO, Brest

- Thomas Genet, jury member (reviewer) for the PhD defense of Lily Gallois, December 2019, Université de Lille

- Alan Schmitt, president of jury for the PhD defense of Florian Dold, February 2019, Université Rennes 1

- Alan Schmitt, jury member (examiner) for the PhD defense of Julien Lopez, September 2019, Université Paris-Saclay

- Alan Schmitt, jury member (reviewer) for the PhD defense of Steven Varoumas, November 2019, Sorbonne Université

- Delphine Demange, jury member (examiner) for the PhD defense of Oscar Luis Vera Pérez, December 2019, Université Rennes 1

- Delphine Demange, member of hiring committee for a Maître de Conférence position, Spring 2019, Lyon 1 / LIP.

## 6.3. Popularization

### 6.3.1. Interventions

- Thomas Genet gave a talk "Bug, Virus, Intrusion, Pirates... So many threats and no defense? Yes... maths." in high schools close to Rennes. 2019.

# CONVECS Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

- H. Garavel is a member of the model board [0] of MCC (*Model Checking Contest*). In 2019, 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'2019 have been published online [44].

- 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, among which 5 were deposited 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.

*10.1.1.2. Member of the Organizing Committees*

- L. Marsso and A. Muroor Nadumane were publicity chairs (also in charge of the conference Web site and social media feeds) for SEFM'2019 (*17th International Conference on Software Engineering and Formal Methods*), Oslo, Norway, September 16–20, 2019.

### 10.1.2. Scientific Events: Selection

*10.1.2.1. Chair of Conference Program Committees*

- G. Salaün was co-chair of SEFM'2019.

*10.1.2.2. Member of the Conference Program Committees*

- H. Garavel was program committee member of FMICS'2019 (*24rd International Conference on Formal Methods for Industrial Critical Systems*), Amsterdam, The Netherlands, August 30–31, 2019.

- R. Mateescu was program committee member of IFIP-ICTSS'2019 (*31st IFIP International Conference on Testing Software and Systems*), Paris, France, October 15–17, 2019.

- G. Salaün was program committee member of SAC-SVT'2019 (*34th ACM Symposium on Applied Computing - Software Verification and Testing Track*), Limassol, Cyprus, April 8–12, 2019.

- G. Salaün was program committee member of FSEN'2019 (*8th IPM International Conference on Fundamentals of Software Engineering*), Tehran, Iran, May 1–3, 2019.

- G. Salaün was program committee member of COORDINATION'2019 (*21st International Conference on Coordination Models and Languages*), Lyngby, Denmark, June 18–21, 2019.

- G. Salaün was program committee member of Microservices'2019, Dortmund, Germany, February 19–21, 2019.

---

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

- G. Salaün was program committee member of COMPSAC-ITIP'2019 and COMPSAC-SETA'2019 (*IEEE International Conference on Computers, Software, and Applications – IT in Practice, and Software Engineering Technologies and Applications*), Wisconsin, USA, July 15–19, 2019.

- G. Salaün was program committee member of HPCS-4PAD'2019 and HPCS-SERCO'2019 (*6th International Symposium on Formal Approaches to Parallel and Distributed Systems, and 3rd Special Session on High Performance Services Computing and Internet Technologies*), Dublin, Ireland, July 15–19, 2019.

- G. Salaün was program committee member of FACS'2019 (*16th International Conference on Formal Aspects of Component Software*), Amsterdam, The Netherlands, October 23–25, 2019.

- G. Salaün was program committee member of FOCLASA'2019 (*17th International Workshop on Coordination and Self-Adaptativeness of Software Applications*), Oslo, Norway, September 17, 2019.

- G. Salaün was program committee member of DATAMOD'2019 (*8th International Symposium "From Data to Models and Back"*), Porto, Portugal, October 7–8, 2019.

*10.1.2.3. Reviewer*

- R. Mateescu was a reviewer for the Festschrift in honor of Stefania Gnesi.

- A. Muroor Nadumane was a reviewer for SAC-SVT'2020, FACS'2019, SEFM'2019, COMPSAC-SETA'2019.

### 10.1.3. Journal

*10.1.3.1. Member of the Editorial Boards*

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

*10.1.3.2. Reviewer - Reviewing Activities*

- F. Lang and A. Muroor Nadumane were reviewers for STTT.

- R. Mateescu was a reviewer for ISSE (*Innovations in Systems and Software Engineering*), IST (*Information and Software Technology*), LMCS (*Logical Methods in Computer Science*), and SCP (*Science of Computer Programming*).

- G. Salaün was a reviewer for JISA (*Journal of Internet Services and Applications*), JLAMP (*Journal of Logical and Algebraic Methods in Programming*), JSME (*Journal of Software: Evolution and Process*), LMCS, and SCP.

### 10.1.4. Software Dissemination and Internet Visibility

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

In 2019, the main facts are the following:

- We prepared and distributed twelve successive versions (2019-a to 2019-l) of CADP.

- We were requested to grant CADP licenses for 340 different computers in the world.

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

By the end of December 2019, the CADP forum [0], opened in 2007 for discussions regarding the CADP toolbox, had over 435 registered users and over 1940 messages had been exchanged.

Also, for the 2019 edition of the Model Checking Contest, one family of models generated using CADP (totalling 16 Nested-Unit Petri Nets) was provided.

---

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

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

- The OCARINA Tool and its Extension AADL2LNT for Analysing AADL Descriptions [49]
- The LFD-MPI Tool for Lightweight Formal Development of MPI Applications [52], [53]
- The FTRES Tool for Rare Event Simulation in Dynamic Fault Trees [54]
- Formal Analysis of Security Guidelines for Program Certification [55]

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

- Applying Automata Learning to Embedded Control Software [50]
- Model Checking Based Approach for Compliance Checking [46]
- Finding Conservative Schema Evolutions by Analysing API Changes [51]
- Selection of Model Checking Strategies using Machine Learning [42]
- Verifying Complex Software Control Systems from Test Objectives [29]
- Designing Safe Synchronous Reactive Systems [30]

## 10.1.5. Invited Talks

- H. Garavel participated in the workshop "*Advancing Verification Competitions as a Scientific Method*" organized by the Lorentz Center (Leiden, The Netherlands) on February 18–22, 2019. He gave a lecture entitled "*Managing Large Collections of Benchmarks: An Experiment Report*".
- H. Garavel presented a retrospective of the Rewrite Engines Competitions at the TOOLympics event at ETAPS 2019, Prague, Czech Republic, April 6–7, 2019.
- H. Garavel was one of the six invited speakers at the panel discussion "*Moore's Law, and More?*" organized at the occasion of the 25th Anniversary of the TACAS conference, Prague, Czech Republic, April 7, 2019.
- H. Garavel gave a highlight talk entitled "*From Safe Petri Nets to NUPNs*" at the 8th IFIP WG 1.8 Workshop on Trends in Concurrency Theory, Amsterdam, The Netherlands, August 31, 2019.
- H. Garavel gave a seminar entitled "*Converting Safe Petri Nets to NUPNs*" at Saarland University, Germany, on September 26, 2019.
- R. Mateescu gave a talk entitled "*The MCL Language for Temporal and Probabilistic Analysis of Concurrent Systems*" at the Languages, Semantics, and Compilation seminar of the LIP laboratory, Lyon, September 19, 2019.
- R. Mateescu visited the Gran Sasso Science Institute (L'Aquila, Italy) on November 4–7, 2019. He gave a talk entitled "*An Action-based Model Checking Language for Concurrent Systems*".
- A. Muroor Nadumane gave a talk entitled "*Advanced Rule-based Composition and Deployment for Web of Things*" at the Inria-Nokia Bell Labs meeting held at Inria Rennes on June 11, 2019.

## 10.1.6. 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, and giving an advice on the recruitment of temporary engineers.
- 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 2019 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.

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

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

In 2019, we carried out the following teaching activities:

P. Bouvier supervised a group of seven two-person teams of 2nd year students in the context of the "*projet informatique*" (31 hours "*équivalent TD*", consisting of lab exercises and supervision) at PHELMA.

H. Garavel was a jury member for the MOSIG master defenses in June and September 2019.

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.

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.

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 250 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 (third year of university) at IUT1/UGA.

W. Serwe gave the part on "*Behavioural Testing*" (9 hours "*équivalent TD*") of the course "*Verification and Test Theories*" to second year students of the MOSIG.

W. Serwe supervised 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 2019.

### 10.2.2. Supervision

PhD: Lina Marsso, "*Formal Methods for Testing Networks of Controllers*", Université Grenoble Alpes, December 10, 2019, R. Mateescu, W. Serwe, and I. Parissis

PhD: Umar Ozeer, "*Autonomic Resilience of Applications in a Largely Distributed Cloud Environment*", Université Grenoble Alpes, December 11, 2019, L. Letondeur, G. Salaün, F.-G. Ottogalli, and J.-M. Vincent

PhD in progress: Pierre Bouvier, "*Implémentation et vérification des langages concurrents de nouvelle génération*", Université Grenoble Alpes, since October 2019, H. Garavel and R. Mateescu

PhD in progress: Ajay Muroor Nadumane, "*Softwarization of Everything: IoT Service Composition*", Université Grenoble Alpes, since October 2017, G. Salaün, R. Mateescu, and M. Le Pallec

### 10.2.3. Juries

- F. Lang was PhD committee member of Sander de Putter's PhD thesis, entitled "*Verification of Concurrent Systems in a Model-Driven Engineering Workflow*", defended at Technische Universiteit Eindhoven (The Netherlands) on January 28, 2019.

- R. Mateescu was reviewer of The Anh Pham's PhD thesis, entitled "*Efficient State-Space Exploration for Asynchronous Distributed Programs*", defended at ENS Rennes on December 6, 2019.

- G. Salaün was committee president of Xavier Etchevers's Habilitation thesis, entitled "*Evolution du déploiement automatisé d'applications : des infrastructures cloud aux enjeux de l'agilité et de l'intelligence ambiante*", defended at Université Grenoble Alpes on November 29, 2019.

- G. Salaün was PhD committee president of Raphaël Jackse's PhD thesis, entitled "*Interactive Runtime Verification*", defended at Université Grenoble Alpes on December 18, 2019.

## 10.3. Popularization

### 10.3.1. Interventions

- R. Mateescu has participated to the "*Journée Transfo : Plongez dans le monde du numérique*" organized at Inria Montbonnot on January 24, 2019.

- R. Mateescu has participated to the "*Fête de la Science*" organized at Inria Montbonnot on October 12, 2019.

## DEDUCTEAM Project-Team

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

#### 9.1.1.1. Member of the Organizing Committees

Deducteam has organized the kick off meeting of Logipedia on 21-23 January 2019 in Cachan.

Frédéric Blanqui and Olivier Hermant organized the 11th International School on Rewriting (ISR) in Paris on 1-6 July 2019. The school offered to 37 participants from 8 countries, 69 hours of lectures in two parallel sessions, given by 15 lecturers from 6 countries.

Valentin Blot co-organized the Facets of realizability workshop on 1-3 July 2019, bringing together 22 researchers from 6 countries.

Frédéric Blanqui is Workshop Chair of the ACM/IEEE Symposium on Logic in Computer Science (LICS).

### 9.1.2. Scientific Events: Selection

#### 9.1.2.1. Member of the Conference Program Committees

Gilles Dowek has been a member of the program committee of the Nasa Formal Methods Symposium (NFM'19) and Interactive Theorem Proving (ITP'19).

Frédéric Blanqui has been member of the program committee of the 16th International Colloquium on Theoretical Aspects of Computing (ICTAC'19), the 6th Workshop on Proof eXchange for Theorem Proving (PxTP'19), and of Large Mathematical Libraries (LML'19).

Valentin Blot was a member of the program committee for the french conference "Journées Francophones des Langages Applicatifs" 2020.

#### 9.1.2.2. Reviewer

Guillaume Burel reviewed articles submitted to PxTP'19 and LOPSTR'19.

Valentin Blot reviewed articles submitted to LICS'19.

Bruno Barras reviewed an article submitted to CSL'20.

### 9.1.3. Journal

#### 9.1.3.1. Reviewer - Reviewing Activities

Guillaume Burel reviewed an article for Logical Methods in Computer Science.

Bruno Barras reviewed articles submitted to the Annals of Mathematics and Artificial Intelligence and Mathematical Structures in Computer Science

### 9.1.4. Invited Talks

Gilles Dowek has been invited to the meeting Big proofs in Edinburgh, where he has given a talk on Logipedia.

Gilles Dowek has participated to the meeting of the Proof society in Swansea where he has given a talk on Logipedia.

Gilles Dowek has given talk on Logipedia in Lille, Strasbourg, Beijing, Rio de Janeiro, and in the virtual "Laboratoire International de Recherche en Informatique et Mathématiques Appliquées".

Frédéric Blanqui gave talks at Gunma University (Japan) and Tohoku University (Japan).

Guillaume Genestier gave a seminar at the logic group of Chalmers University (Sweden).

Valentin Blot gave an invited talk at a realizability workshop on 18-20 September 2019 in Marseille, and a talk at the IRIF semantics working group.

### 9.1.5. Leadership within the Scientific Community

Frédéric Blanqui is member of the Steering Committees of LICS, TYPES and ISR.

### 9.1.6. Scientific Expertise

Bruno Barras reviewed a research proposal submitted to the Dutch National Research Organization (NWO).

### 9.1.7. Research Administration

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. Teaching - Supervision - Juries

### 9.2.1. Teaching

- Master: Frédéric Blanqui, formal languages, 21h, M1, ENSIIE, France
- Master: Frédéric Blanqui, rewriting theory, 14h, M1, ENS Paris-Saclay, France
- Master: Frédéric Blanqui, $\lambda$-calculus and theories in first-order logic, 18h, M1/M2, ENS Paris-Saclay, France
- Master: Bruno Barras, Proof Assistants, 12h, M2, MPRI, France
- Master: Gabriel Hondet, rewriting theory TD, 14h, M!, ENS Paris-Saclay, France
- Licence: Gabriel Hondet, operating systems and architecture TD, 22.5h, L3, ENS Paris-Saclay, France
- Licence: Gabriel Hondet, programming TD, 12h, L3, ENS Paris-Saclay, France
- License: Gaspard Férey, Théorie des Langages, 44h, L3, EISTI
- IUT: Yacine El Haddad, Programmation Web Côté Serveur, 62h, IUT of Orsay

### 9.2.2. Supervision

- 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: Gabriel Hondet, translating PVS proofs to Dedukti, 01/10/19, Frédéric Blanqui and Gilles Dowek.

### 9.2.3. Juries

Bruno Barras and Valentin Blot have participated to the PhD jury of Youssef El Bakouny from Université St-Joseph, Beirut (Lebanon).

## 9.3. Popularization

### 9.3.1. Articles and contents

Articles

- The synthesis article Algorithmes et modèles : l'histoire d'une convergence, written a decade ago has been published in Pierre Mounoud, Leçons de mathématiques d'aujourd'hui : Volume 5 (Cassini,2019).

Books

- Gilles Dowek, Ce dont on ne peut parler, il faut l'écrire : Langues et langages (Le Pommier, 2019)

Manuscripts

- Gilles Dowek, How the physical Church-Turing thesis changed the concept of machine, manuscript, 2019.
- Gilles Dowek, Two consequences of the hypothesis that we are within the world, manuscript, 2019.
- Gilles Dowek, Instinct, language, and artificial intelligence, manuscript, 2019.

### 9.3.2. Interventions

Gilles Dowek has been invited to the PROGRAMme workshop "Machines" where he has presented a paper How the physical Church-Turing thesis changed the concept of machine.

Gilles Dowek has been invited to the Conference on Robotics, AI, and Humanity, Science, Ethics, and Policy organized by the Pontifical Academy of Sciences and the Pontifical Academy of Social Sciences where he has presented a paper Instinct, language, and artificial intelligence.

Gilles Dowek has been invited at the meeting Le hasard, le calcul et la vie, in Cerisy, where he has given a talk Un Chaos discret.

Gilles Dowek has been invited to the meeting Experiencing reality directly in Jerusalem where he has presented a paper Two consequences of the hypothesis that we are within the world.

# GALLINETTE Project-Team

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Selection

*8.1.1.1. Chair of Conference Program Committees*

- A. Mahboubi has served as co-PC chair of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP'19).
- A. Mahboubi has served as co-chair of the CoqPL'20 workshop, satellite of POPL'20.

*8.1.1.2. Member of the Conference Program Committees*

- P.-M. Pédrot has been a member of the program committee of the Coq Workshop'19 and JFLA'20.
- N. Tabareau has been a member of the program committee of FSCD'19 and POPL'19.
- G. Munch-Maccagnoni has been a member of the external review committee for ICFP'19 conference, and a member of the program committees for the workshops SD'19 (affiliated with FSCD) and LOLA'19 (affilitated with LICS).
- A. Mahboubi has been a member of the program commitee of the ITP'19, Frocos'19 and CPP'20 international conferences, and of the TFP'19 workshop.
- G. Jaber has been a member of the program committee of the Student Research Competition of POPL'20.

*8.1.1.3. Reviewer*

- P.-M. Pédrot has served as an external reviewer for CPP'19, FoSSaCS'19, ICFP'19 and LICS'19.
- N. Tabareau has served as an external reviewer for LICS'19, CPP'19.
- G. Munch-Maccagnoni has served as an external reviewer for FoSSaCS'20.
- G. Jaber has served as an external reviewer for CONCUR'19, ITP'19, FoSSaCS'19 and POPL'20.

### 8.1.2. Journal

*8.1.2.1. Member of the Editorial Boards*

- A. Mahboubi is a member of the editorial board of the Journal of Automated Reasoning.
- A. Mahboubi is co-editing the post-proceedings of the TYPES 2019 conference.

*8.1.2.2. Reviewer - Reviewing Activities*

- N. Tabareau has been a reviewer for Mathematical Strucutre in Computer Science.

### 8.1.3. Invited Talks

- P.-M. Pédrot gave a 3 hour long invited class on effectful types theories at the JFLA 2019.
- N. Tabareau has given an invited talk at Coq Workshop 2019 in Portland, Oregon.
- G. Munch-Maccagnoni gave a talk at ITU Copenhaguen in July and a talk at the seminar of philosophy in computer science Codes Sources in Paris in June.
- A. Mahboubi has given an invited talk repectively at the MPC'19, CiE'19, Cade'19 and Types'19 international conferences, at the PxTP'19 international workshop and at the Codes Sources seminar.

### 8.1.4. Leadership within the Scientific Community

- N. Tabareau is a member of the scientific committee of the GdR of Algebraic Topology.

- A. Mahboubi is a member of the core managment group of the EUTypes project, and leader of the "Tools" working group.
- A. Mahboubi is a member of the steering committee of the ITP conference.
- A. Mahboubi is a member of the scientific committee of the GdR "Informatique Mathématique".

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

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

Licence : Julien Cohen, Introduction to proof assistants (Coq), 8h, L2 (PEIP : IUT/Engineering school), Polytech Nantes, France

Licence : Julien Cohen, Functional Programming (Scala), 22h, L2 (IUT), IUT Nantes, France

Master : Julien Cohen, Object oriented programming (Java), 32h, M1 (Engineering school), Polytech Nantes, France

Master : Julien Cohen, Functional programming (OCaml), 18h, M1 (Engineering school), Polytech Nantes, France

Master : Julien Cohen, Tools for softaware engineering (proof with Frama-C, test, code management), 20h, M1 (Engineering school), Polytech Nantes, France

Licence : Rémi Douence, Object Oriented Design and Programming, 45h, L1 (engineers), IMT-Atlantique, Nantes, France

Licence : Rémi Douence, Introduction to scientific research in computer science (Project: an Haskell interpreter in Java) Project, 20h, L1 (engineers), IMT-Atlantique, Nantes, France

Licence : Rémi Douence, Object Oriented Design and Programming Project, 30h, L1 (apprenticeship), 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

Licence : Hervé Grall, Algorithms and Discrete Mathematics, 25h , L3 (engineers), IMT-Atlantique, Nantes, France

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

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

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

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

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

Master : Guilhem Jaber, Verification and Formal Proofs, 18h, M1, Université de Nantes, France

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

### 8.2.2. Supervision

PhD : 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 : 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: Joachim Hotonnier, Deep Specification for Domain-Specific Modelling, advisors: Gerson Sunye (Naomod team), Massimo Tisi (Naomod team), Hervé Grall

PhD in progress: Igor Zhirkov, Certified Refactoring of C in the Coq proof assistant, advisors: Rémi Douence and Julien Cohen.

##### 8.2.2.1. Supervision of interns

E. Bauer has visited the team for an L3 research internship from June to July on the subject "Categorical models of differential linear logic", supervised by Marie Kerjean.

A. Ben Mansour has visited the team for an L3 research internship from June to August on the subject "Parametricity for languages with effects", supervised by G. Munch-Maccagnoni.

M. Bertrand has visited the team from February to July for an internship on the subject "Effects in Type Theory", supervised by N. Tabareau.

L. Pujet has visited the team from April to August for an internship on the subject "Interpreting Cubical Type Theory using forcing", supervised by N. Tabareau.

G. Combette is visiting the team from October 2019 to February 2020 for an internship on the subject "Axiomatic denotational semantics for resource management in systems programming", supervised by G. Munch-Maccagnoni.

L. Escot has visited the team from October to December for an internship on the subject "Univalent Parametricity at Scale", supervised by N. Tabareau.

P. Geneau de Lamarlière has visited the team for an L3 research internship from June to July on the subject "Symbolic computations in algebraic number theory", co-supervised by A. Mahboubi and S. Dahmen (VU Amsterdam).

### 8.2.3. Juries

- N. Tabareau has served as external member on the PhD jury of Kenji Maillard, defended November 25th at Inria Paris - Université Paris Sciences et Lettres.

- A. Mahboubi has served as external member on the PhD jury of Florian Faissole, defended December 13th at Paris Saclay University.

- A. Mahboubi has served as external member on the PhD jury of Gaëtan Gilbert, defended December 20th at IMT Atlantique.

- A. Mahboubi has served on the 2019 jury for recruiting Inria CRCN at Inria Rennes Bretagne Atlantique.

- A. Mahboubi has served on the 2019 jury for recruiting an "Agrégé Préparateur" at ENS Rennes.

## 8.3. Popularization

### 8.3.1. Education

- Hervé Grall has contributed to the project Merite, which aims to promote science learning in middle and high schools. He is the main contributor to the theme "Communication between machines". The project is coordinated by IMT-Atlantique in partnership with 7 other french higher education institutions, the rectorates of the Nantes and Rennes academies, and financed by the "Investments in the Future" and the fund FEDER Pays-de-la-Loire.

- A. Mahboubi has worked with composer Alessandro Bossetti and students of the professional high-school Lycée Michelet, on a project "Art and Mathematics", supported by the Athenor theater.

### 8.3.2. Interventions

- P.-M. Pédrot was invited to give a talk about his scientific activities in Le Pleynet, during the "Semaine Sport-Études" of the first year students in computer science from the ENS Lyon.
- P.-M. Pédrot gave a similar talk about his scientific activities at the LS2N, during the visit of first year students in computer science from the ENS Cachan.

### 8.3.3. Internal action

- A. Mahboubi participates to the Irisa/Inria mentoring program.

<h1 style="text-align:center; color:red;">MEXICO Project-Team</h1>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. General Chair, Scientific Chair*

- Serge Haddad is a member of the stering committee of the International Conference on Application and Theory of Petri Nets and Concurrency.

- PHILIPPE DAGUE co-organized with Franck Delaplace the conference on *Computational Systems Biology for Complex Diseases* on November 28-29, 2019 at ENS Paris-Saclay, which gathered around 80 participants.

- PHILIPPE DAGUE, as responsible of the working group BIOSS-IA (Systemic Symbolic Biology and Artificial Intelligence) of the GDR IA, organized the 2019 Day at Orléans on May 27.

- MATTHIAS FUEGGER co-organized the CELLS workshop at DISC'19. The workshop covers topics from computing among a consortium of cells.

- STEFAN HAAR co-directed with Benedikt Bollig the scientific and logistic organisation of the ForMal workshop at ENS Paris-Saclay on cross-fertilization between formal methods and machine learning.

*9.1.1.2. Member of the Organizing Committees*

- STEFAN HAAR was co-chair and SERGE HADDAD was a member of the Scientific Committee (including organisational issues) of the Digicosme Spring School on Formal Methods and Machine Learning held in June at Cachan *(ForMaL)*.

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Chair of Conference Program Committees*

- STEFAN HAAR was co-chair of program committee for the *40th International Conference on Application and Theory of Petri Nets and Concurrency*, Aachen, Germany, June 23-28, 2019.

*9.1.2.2. Member of the Conference Program Committees*

- Serge Haddad was a member of the PC of
    - the workshop PNSE associated with ATPN 2019, Aachen, Germany, and
    - the 12th International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS 2019), Palma de Mallorca, Spain.

- PHILIPPE DAGUE was a member of the program committee of the *30th International Workshop on Principles of Diagnosis DX'19*, Klagenfurt/Austria, November 2019.

- STEFAN HAAR was
    - a member of the programm committee of the *19th International Conference on Applications of Concurrency to Systems Design (ACSD 2019)*, Aachen, Germany, June 23-28, 2019, and
    - a member of the program committee of the *Workshop Algorithms & Theories for the Analysis of Event Data 2019 (ATAED 2019)*.

- MATTHIAS FUEGGER was
    - Steering commitee member of IEEE ASYNC'19 and
    - PC member of IEEE ASYNC'19 and IEEE DDECS'19.

- THOMAS CHATAIN was
  - a member of the programm committee of the *19th International Conference on Applications of Concurrency to Systems Design* (ACSD 2019), Aachen, Germany, June 23-28, 2019, and
  - a member of the program committee of the *1st International Conference on Process Mining (ICPM 2019)*
- LINA YE was a member of the program committee of the *17th International Workshop on Coordination and Self-adaptativeness of Software Applications* (FOCLASA 2019).
- Stefan Schwoon acted as reviewer for MFCS 2019, FSTTCS 2019, FOSSACS 2019,, TACAS 2019, and STACS 2020.
- LINA YE was
  - a reviewer of the *58th Conference on Decision and Control* (CDC 2019), and
  - a reviewer of the *the 30th International Workshop on Principles of Diagnosis* (DX 2019).

### 9.1.3. Journal

*9.1.3.1. Member of the Editorial Boards*

- STEFAN HAAR is an associate editor for *Journal of Discrete Events Dynamic Systems: Theory and Application* (JDEDS).

*9.1.3.2. Reviewer - Reviewing Activities*

- Serge Haddad was a reviewer for the following journals:
  - Journal of Logical and Algebraic Methods in Programming,
  - Innovations in Systems and Software Engineering, and
  - Transactions on Petri Nets and Other Models of Concurrency.
- Thomas Chatain was a reviewer for journals *Journal of Discrete Events Dynamic Systems: Theory and Application* (JDEDS) and Fundamenta Informaticae.
- Stefan Schwoon was a reviewer for *Journal of Discrete Event Dynamic Systems* (JDEDS), *Transactions on Software Engineering* (TSE), *Petri Nets and Other Models of Concurrency* (ToPNoC), and Transactions on Programming Languages and Systems (TOPLAS).
- LINA YE is a reviewer for *Journal of IEEE Access* (IEEE Access).

### 9.1.4. Invited Talks

- Stefan Schwoon gave a talk in the SYBILA seminar of Masaryk University, Brno, on *Diagnosis and Opacity in Partially Observable Systems*.

### 9.1.5. Scientific Expertise

- Serge Haddad is a member of the scientific and administrative council (CSA) of Labex CIMI of Toulouse and a member of the scientific orientation council (COS) of LIS of Marseille (UMR 7020).

### 9.1.6. Research Administration

- Serge Haddad is Head of the Computer Science Department of ENS Paris-Saclay.
- Stefan Haar is the president of Inria's COST-GTRI.

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

- MATHIAS FUEGGER,

    Master :

– *Initiation à la recherche*, 10 h EQTD, M1, ENS Paris-Saclay, France

- STEFAN HAAR,

    Licence : *Langages Formels*, EQTD, L3, ENS Paris-Saclay, France;

    Master :

    – *Analyse de la dynamique des systèmes biologiques*, 10 h EQTD, M1, Université PAris-Saclay, France

    – *Initiation à la recherche*, 10 h EQTD, M1, ENS Paris-Saclay, France

    – *Module SPECIF* , 12 h EQTD, M1, UPMC, France.

    Serge Haddad is head of the Computer Science department of ENS Paris-Saclay. He teaches basic and advanced algorithmics (L3) and probabilistic features of computer science (M1).

    STEFAN SCHWOON

    – Responsable L3 Informatique, ENS Paris-Saclay

    – Enseignement au M1 MPRI : cours *Initiation à la Vérification* (22,5h)

    – Enseignement au L3 Info : cours *Architecture et Système* (45h), projet *Programmation orienté objet* (15h), TD *Langages Formels* (22,5h)

    – Enseignement à l'Aggrétation Maths Option Informatique: cours *Algorithmique* (22,5h)

### 9.2.2. Supervision

- SERGE HADDAD is supervising with Alain Finkel the PhD thesis of Igor Khmelnitsky on Verification of infinite-state systems and machine learning.

- STEFAN HAAR has been supervising, with Co-supervisor Loic Paulevé at LABRI, the PhD theses of

    HUGUES MANDON, *Models and Algorithms for cellular reprogramming strategies prediction*, ENS Paris-Saclay, defended on Nov. 19, 2019, and

    JURAJ KOLCˇÁK, *Parametric Logical Regulatory Networks*, PhD research started in March 2017.

- THOMAS CHATAIN has been supervising, with co-superviser Josep Carmona at Universitat Politècnica de Catalunya (Barcelona, Spain), the PhD thesis of MATHILDE BOLTENHAGEN, *Optimization Techniques for Conformance Checking and Model Repair in Process Mining*, PhD research started in November 2018.

- LINA YE has been supervising, with Co-superviser Philippe Dague at LRI, the PhD these of LULU HE, *Robustness Analysis of Real-Time Systems*, PhD research started in February 2019.

### 9.2.3. Juries

- PHILIPPE DAGUE was *garant* and member of the HdR jury of Sabine Peres, and a member of the HdR jury of Jean-Marie Lagniez.

- Serge Haddad was the president of the PhD committee of Mauricio Gonzalez defended at ENS Paris-Saclay in November.

- THOMAS CHATAIN has been a jury member for the PhD defense of SAMY JAZIRI (supervisers Patricia Bouyer-Decitre et Nicolas Markey) at Université Paris-Saclay in September 2019.

- THOMAS CHATAIN has been a jury member for the SIF PhD award (Prix de thèse Gilles Kahn 2019).

## 9.3. Popularization

### 9.3.1. Internal or external Inria responsibilities

- STEFAN HAAR has been the president of COST-GTRI.

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. General Chair, Scientific Chair*

- Mathieu Hoyrup was chair and organizer of the workshop MLA 2019.
- Jointly with Andreas Deutsch (TU Dresden, Germany), Nazim Fatès was chair and organizer of SOLSTICE 2019, Summer Solstice Conference on Discrete Models of Complex Systems.

*9.1.1.2. Member of the Conference Program Committees*

- Mathieu Hoyrup was member of the PC of CiE 2019.
- Romain Péchoux was member of the PC of DICE and FOPARA 2019.
- Nazim Fatès was member of the PC of AUTOMATA 2019.
- Simon Perdrix was member of the PC of QPL'19.

*9.1.1.3. Reviewer*

Romain Péchoux was reviewer for DICE and FOPARA 2019, FOSSACS 2019, ICALP 2019, and ISMVL 2019.

### 9.1.2. Journal

*9.1.2.1. Member of the Editorial Boards*

- Emmanuel Jeandel is member of the Editorial Board of RAIRO-ITA.
- Nazim Fatès is a member of the Editorial board of the *Journal of cellular automata*.

*9.1.2.2. Reviewer - Reviewing Activities*

- Romain Péchoux was reviewer for Information Processing Letters and Journal of Automated Reasoning.
- Nazim Fatès served as a reviewer for the *SIAM Journal on Discrete Mathematics* (SIDMA) and for *Informatica*.

### 9.1.3. Invited Talks

Romain Péchoux gave an invited talk at Shonan seminar #151 on higher order complexity theory and its applications.

### 9.1.4. Leadership within the Scientific Community

- Romain Péchoux is guest coeditor of the Theoretical Computer Science, special issue on Implicit Computational Complexity, DICE 2016-2018.
- Nazim Fatès is the vice-president of the IFIP WG 1.5 on Cellular Automata and Discrete Complex Systems. He is a guest coeditor of a special issue of *Natural computing* on the theme "Discrete Models of Complex Systems: recent trends and analytical challenges". This call for papers follows the SOLSTICE 2019 conference (Dresden, Germany, July 2019).

### 9.1.5. Scientific Expertise

- Romain Péchoux is Rapporteur and Expert for the Marie Curie IF call of the European Commission, ERA.
- Nazim Fatès was an evaluator for a funding project of the CONICYT, the Chilean *Comisión Nacional de Investigación Científica y Tecnológica*.
- Simon Perdrix was member of the HCERES evaluation committee of G-SCOP.
- Simon Perdrix was member of the committee "La Recherche" award (Prix du Magazine La Recherche) 2019.

### 9.1.6. Research Administration

- Emmanuel Hainry was member of the CNU (Conseil National des Universités), Section 27 until 2019, nov 18th.
- Simon Perdrix is elected member and scientific secretary of the CNRS section 6.

## 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", Université de Lorraine, Nancy, France.
  - Emmanuel Hainry:
    * Operating Systems, 30h, L1, IUT Nancy Brabois, Université de Lorraine, Nancy, France.
    * 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.
  - Emmanuel Jeandel:
    * Algorithmics and Programming 1, 60h, L1 Maths-Info, Université de Lorraine, Nancy, France.
    * Algorithmics and Programming 4, 30h, L3 Informatique.
    * Modeling Using Graph Theory, 30h, L3 Informatique.
    * Networking, 15h, L3 Informatique.
    * Formal Languages, 30h, L2-L3 Informatique.
  - Romain Péchoux had an Inria delegation (2018-2019).
- Master

– Isabelle Gnaedig:

* Rule-based Programming, 24 hours, M2, Telecom-Nancy, Université de Lorraine, Nancy, France.

– Emmanuel Hainry:

* Mathematics for Computer Science, 15h, M1 TAL, Institut des Sciences du Digital: Management et Cognition, Université de Lorraine, Nancy, France.

– Mathieu Hoyrup:

* Mathematics for Computer Science, 15h, M1 TAL, Institut des Sciences du Digital: Management et Cognition, Université de Lorraine, Nancy, France.

– Emmanuel Jeandel:

* Algorithmics and Complexity, 30h, M1 Informatique, Université de Lorraine, Nancy, France.

* Quantum Computing, 15h, M1 Informatique.

– Nazim Fatès:

* Systèmes distribués adaptatifs, 10h, Master 2, informatique, Université de Lorraine, Nancy, France.

* Agents intelligents et collectifs, 15h, Master 1, sciences cognitives.

* Modèles de calcul, 12h, Master 2, informatique.

## 9.2.2. Supervision

- Mathieu Hoyrup supervised the L3 internship of Antonin Callard (ENS Paris Saclay), about descriptive set theory on represented spaces.

- Emmanuel Hainry and Romain Péchoux supervised the L3 internship of Olivier Zeyen (FST, Université de Lorraine), on implementing a complexity parser for Java.

- Nazim Fatès supervised the internship of Karim Boutamine and Maxime Thaon, students of Master 1 in Cognitive Sciences (Université de Lorraine) and the internship of Baptiste Collet, student of Licence 3 at École normale supérieure de Paris.

- PhD: Renaud Vilmart, "Langages graphiques pour calculer et raisonner en quantique", defended september 2019, 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.

- PhD in progress: Alexandre Clément, "Graphical Languages for Quantum Control", Start: September 2019, Advisors: Emmanuel Jeandel and Simon Perdrix.

- PhD in progress: Margarita Veshchezerova, "Quantum Computing for Combinatorial Optimisation", Start: October 2019, Advisors: Emmanuel Jeandel and Simon Perdrix, joint supervision with Marc Porcheron at EDF (CIFRE).

## 9.2.3. Juries

- Emmanuel Jeandel participated in the PhD defense of Florian Bridoux (Université d'Aix-Marseille), François Pirot (Université de Lorraine and Rahdboud University) and Alexandre Talon (ENS Lyon).

- Emmanuel Jeandel reviewed the PhD thesis of Paulina Cecchi (University of Santiago and Université Paris-Diderot) and Ilya Galanov (Université de Villetaneuse).

- Nazim Fatès reviewed the PhD of Adam Dzedzej (University of Gdańsk, Poland) and served a the main external examiner during the PhD defense.

- Simon Perdrix was external reviewer for the PhD thesis of Kang Feng Ng (Oxford University), March 2019.

- Simon Perdrix was reviewer for the PhD thesis of Matthew Amy (University of Waterloo, Canada), January 2019.

- Simon Perdrix reviewed the PhD thesis of Ghazal Kachigar (University of Bordeaux), December 2019.

## 9.3. Popularization

### 9.3.1. Articles and contents

- The scientific magazine *La Recherche* re-published an article by Nazim Fatès and Irène Marcovici, with the title "Les automates cellulaires jouent le jeu", in a Special issue devoted to the theme "Les maths et le réel" (September 2019) [34]. The original article "Automates cellulaires : la complexité dans les règles de l'art" (2018), was modified with minor changes for this special issue.

- Interviews of Simon Perdrix about the Google's result on quantum advantage. La tribune (online article) ; Sciences et Avenir (November 2019 - paper journal and online articles), We demain (online article).

### 9.3.2. Education

Nazim Fatès participated to a workshop destined to the high-school teachers which were training on the « Information et sciences du numérique » module.

In the lycée Saint-Exupéry de Saint-Dizier: he gave three one-hour conferences destined to students, related to the film *Imitation game* on Alan Turing (March 18).

### 9.3.3. Interventions

Nazim Fatès was invited to give various talks on the question of artificial intelligence:

- With the European parliamentary association (APE), he was invited to talk to European MP's on the the theme « Is Europe ready for artificial intelligence? » (Strasbourg, February 13).

- In the « Sciences et société » cycle of IUT Charlemagne (September 26).

- With the association « Jardin des sciences », cycle « intelligences » destined to a wide public, University of Strasbourg (October 10).

- With the association Femmes responsables (November 20).

<span style="color:red">**PARSIFAL Project-Team**</span>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

Dale Miller is currently General Chair for the ACM/IEEE Symposium on Logic in Computer Science (LICS).

*10.1.1.2. Member of the Organizing Committees*

Dale Miller is member of the Steering Committee for CPP, FSCD, and LFMTP and is a member of the Executive Committee of the ACM Special Interest Group on Logic and Compuation (SIGLOG).

Gabriel Scherer is part of the Steering Committee of the ML Family Workshop and the OCaml Workshop.

### 10.1.2. Scientific Events: Selection

*10.1.2.1. Chair of Conference Program Committees*

Dale Miller was program committee co-chair for the workshop on Logical Frameworks and Meta Languages: Theory and Practice (LFMTP), 2019, Vancouver, Canada.

*10.1.2.2. Member of the Conference Program Committees*

- Gabriel Scherer: JFLA 2020.
- Beniamino Accattoli: LSFA 2019.
- Dale Miller is a PC member for the 10th International Joint Conference on Automated Reasoning (IJCAR-2020), the 23rd International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR-23), and the Workshop on Trends, Extensions, Applications and Semantics of Logic Programming (TEASE-LP).

*10.1.2.3. Reviewer*

- Gabriel Scherer: POPL 2020, ESOP 2020.
- Lutz Straßburger: FoSSaCS 2020, CSL 2020, TABLEAUX 2019, WoLLIC 2019, LICS 2019.
- Beniamino Accattoli: FoSSaCS 2020, POPL 2020, ICALP 2019, ICTAC 2019, PPDP 2019, FSCD 2019, CSL 2019, LSFA 2019.

### 10.1.3. Journal

*10.1.3.1. Member of the Editorial Boards*

Dale Miller is on the editorial board of the Journal of Automated Reasoning (Springer) and the Jounral of Applied Logic (Elsevier). He has also been an editor for a special issue of FSCD 2017 for Logical Methods in Computer Science.

*10.1.3.2. Reviewer - Reviewing Activities*

- Lutz Straßburger: APAL, ToCL, BSL, LMCS.
- Beniamino Accattoli: LMCS, TCS.
- Dale Miller has served on the evaluation committee for the EATCS Distinguished Dissertation Award and the EACSL Ackermann Award. He was also the Chair of the Herbrand Award Committee of the Association for Automated Reasoning.

### 10.1.4. Invited Talks

- Beniamino Accattoli has been invited speaker at FSCD 2019.
- Dale Miller has been an invited speaker at the Workshop on Proof Theory for Automated Deduction, Automated Deduction for Proof Theory (23-25 October 2019, Funchal, Madeira) and the Third Tübingen Conference on Proof-Theoretic Semantics, 27-30 March 2019.

### 10.1.5. Scientific Expertise

- Lutz Straßburger: reviewer for the Israel Science Foundation.
- Dale Miller has been a member of an international review panel for the Distinguished Professor Grant at the Swedish Research Council.
- Gabriel Scherer: reviewer for ANR.

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Licence : G. Scherer, "*Introduction á la programmation fonctionnelle*", 50h, L1, Paris 8 (Vincennes - Saint Denis), France

Master: B. Accattoli, "*Logique linéaire et paradigmes logiques du calcul*", 18h, M2, Master Parisien de Recherche en Informatique (MPRI), France.

Master: D. Miller, "*Logique linéaire et paradigmes logiques du calcul*", 18h, M2, Master Parisien de Recherche en Informatique (MPRI), France.

Summer School: G. Scherer, "*Programmation fonctionnelle en OCaml*", 12h, public d'ingénieurs de recherche, formation ANF (CNRS), France

Summer School: L. Straßburger: "*Introduction to Deep Inference*", 10h, ESSLLI 2020, Riga, Latvia

Summer School: B. Accattoli, "*λ-Calculus and Reasonable Cost Models*", 15h, Escuela de Ciencia Informaticas (ECI 2019), Buenos Aires, Argentina.

### 10.2.2. Supervision

- PhD in progress: Marianela Morales, "Combinatorial Proof Theory for Modal Logic", 1/10/2019, Lutz Straßburger.
- PhD in progress: Maico Leberle, "Call-by-need and Reasonable Cost Models", Beniamino Accattoli.
- PhD completed: Ulysse Gérard, "Computing with relations, functions, and bindings", 18 October 2019, Ecole Doctorale de l'Institut Polytechnique de Paris, advised by Dale Miller.
- PhD in progress: Matteo Manighetti, "Structural proof theory for induction in linear logic", advised by Dale Miller since 1/10/2017.
- PhD in progress: Marianela Morales, "Combinatorial Proof Theory for Modal Logic", 1/10/2019, Lutz Straßburger

### 10.2.3. Juries

Dale Miller was a reportor for the PhD thesis of Aurore Alcolei (ENS Lyon, 17 October 2019).

## 10.3. Popularization

### 10.3.1. Interventions

G. Scherer and M. Manighetti participated the "Fête de la Science" exhibit at Inria Saclay on the whole day of October 11th, 2019.

G. Scherer presented the research domain of certified programming to an audience of computer security professionals at the "Pass the Salt" conference in Lille, on Wednesday July 3rd.

# PI.R2 Project-Team

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

*9.1.1.1. Member of the Organizing Committees*

Alexis Saurin, as coordinator of GT-Scalp is member of the organizing committee of the annual meeting of the working group. In 2019, the annual meeting took place in ENS Lyon in October 2019: https://www.irif.fr/gt-scalp/journees-2019.

*9.1.1.2. Member of the Steering Committees*

Pierre-Louis Curien is member of the steering committee of the international workshop Games for Logic and Programming Languages (GaLop).

### 9.1.2. Scientific Events: Selection

*9.1.2.1. Member of the Conference Program Committees*

Pierre-Louis Curien is member of the program committee of Formal Structures for Computation and Deduction 2020, Paris, June-July 2020.

Yann Régis-Gianas was member of the program committee of Software Language Engineering 2019.

Alexis Saurin was a member of the program committee of Circularity in Syntax and Semantics, held in Gothenbug in November 2019.

### 9.1.3. Journal

*9.1.3.1. 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 a guest editor of the special issue of MSCS on structural proof theory, automated reasoning and computation in celebration of Dale Miller's 60th birthday published in September 2019.

*9.1.3.2. Reviewer - Reviewing Activities*

Pierre Letouzey has done several reviews for the Journal of Functional Programming (JFP) and for Science of Computer Programming. Yann Régis-Gianas reviewed a paper for Transactions on Programming Languages and Systems (TOPLAS).

### 9.1.4. Invited Talks

Hugo Herbelin gave an invited talk on the logical structure of choice and bar induction principles at the Proof, Computation and Complexity workshop (Mittag-Leffler institute). Yann Régis-Gianas gave an invited talk at the DeepSpec workshop of PLDI 2019 about FreeSpec.

### 9.1.5. Conferences and schools attended

Pierre-Louis Curien presented his joint work on Proofs and surfaces at the conference Topology, Algebra, and Categories in Logic (TACL) 2019, Nice, in June 2019.

Pierre-Louis Curien and Yves Guiraud attended the workshop Homotopy meets homology, Dublin, May 2019.

Pierre-Louis Curien and Yves Guiraud attended the *Higher Structures* conference, Marseille, January 2019.

Pierre-Louis Curien and Cédric Ho Thanh attended the Category Theory 2019 conference, Edinburgh, July 2019.

Pierre-Louis Curien attended Martin Hofmann Memorial Meeting, Munich, July 2019.

Abhishek De attended the Proof Society summer school at Swansea in September 2019.

Cédric Ho Thanh attended the Summer school on Topology, Algebra, and Categories in Logic at Ile de Porquerolles in June 2019.

Hugo Herbelin and Hugo Moeneclaey attended the Types Conference, Oslo, June 2019.

Hugo Moeneclaey attended the International Conference on Homotopy Type Theory (HoTT 2019) and the associated Homotopy Type Theory Summer School, Pittsburgh, August 2019.

Hugo Herbelin attended the Third Workshop on Mathematical Logic and its Applications, Nancy, March 2019.

Hugo Herbelin attended the Workshop Facets of Realizability, Cachan, July 2019.

### 9.1.6. Leadership within the Scientific Community

#### 9.1.6.1. Scientific Expertise

Hugo Herbelin was a member of the HCERES committee evaluating the MICS laboratory of Centrale Supelec.

#### 9.1.6.2. Research Administration

Pierre-Louis Curien has been a member of the Scientific Council of the CIRM (Centre International de Rencontres Mathématiques) until February 2019.

Pierre-Louis Curien was a member of the scientific council of the Computer Science department of University Paris Diderot until May 2019.

Yves Guiraud was the coordinator of the Proofs, Programs and Systems (PPS) pole at IRIF, and a member of the IRIF comité de direction, until August 2019. Since September 2019, Hugo Herbelin coordinates the PPS pole.

Yves Guiraud was a member of the Conseil Scientifique of the CS department of Univ. Paris Diderot until June 2019.

Yves Guiraud is a member of the Conseil Scientifique of the Math department of Univ. Paris Diderot since April 2019.

Alexis Saurin is a coordinator of the Scalp working group of GDR Informatique Mathématique: https://www.irif.fr/gt-scalp/index

Alexis Saurin is member of the "commission recherche" of both Faculté des Sciences and Faculté Société et humanités at Université de Paris.

Alexis Saurin and Hugo Herbelin are members of the IRIF conseil de laboratoire.

# 9.2. Teaching - Supervision - Juries

## 9.2.1. Teaching

- Master: Matthieu Sozeau, Assistants de Preuve, 18h ETD, MPRI, University Paris Diderot.
- Master: Pierre-Louis Curien, Models of programming languages: domains, categories, games (together with Thomas Ehrhard and Paul-André Melliès), 15h, MPRI, University Paris Diderot.
- Master level: Pierre-Louis Curien taught a course on the Foundations of Programming Languages at East China Normal University (4 hours, November-December 2019).
- Master: Hugo Herbelin taught a class on Homotopy Type Theory (together with Nicolas Tabareau), 24h, LMFI, University Paris Diderot.
- Master: Pierre Letousey 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 Letousey's regular duty as teacher in the Computer Science department of University Paris Diderot (including a course on Compilation to M2-Pro students and a course on computed-aided formal proofs to M1 students).

- Master: Yann Régis-Gianas, Functional programming and Type Systems, 12h, MPRI (in addition to four other courses at the master level in University Paris Diderot).

- Master: Alexis Saurin, Outils classiques pour la correspondance de Curry-Howard, 24H, LMFI.

- Summer school: Pierre-Louis Curien gave an introductory mini-course on Homotopy type theory at the Fifteenth International Tbilisi Summer School in Logic and Language, Georgia, in September 2019 (3h).

- Summer school: Hugo Herbelin gave a lecture on type theory at the EUTypes Summer School, Ohrid, in September 2019 (4h).

- Yann Régis-Gianas organised the 4th session of the OCaml MOOC on the FUN platform.

- Yann Régis-Gianas organised the "Journée Francilienne de Programmation", a programming contest between the first years students of University Paris Sorbonne, University Paris Saclay and University Paris Diderot.

### 9.2.2. Supervision

*9.2.2.1. PhD Supervision*

- PhD started: Félix Castro, Computational contents of the model of constructible sets, cotutelle between Université Paris Diderot and Universidad de la República (Montevideo, Uruguay), started in September 2019, supervised by Hugo Herbelin and Alexandre Miquel.

- PhD Started: Kostia Chardonnet, Inductive and coinductive types in quantum programming languages, Université Paris Saclay, started in November 2019, supervised by Alexis Saurin and Benoît Valiron.

- PhD started: Alen Durić, Normalisation for monoids and higher categories, Université Paris Diderot, started in October 2O19, supervised by Yves Guiraud and Pierre-Louis Curien.

- PhD started: Colin Gonzalez, Certified compilation of spreadsheets as Tezos smart contract, CIFRE, started in September 2019, supervised by Yann Régis-Gianas and Benjamin Canou (Nomadic Labs).

- PhD started: Farzad Jafar-Rahmani, Denotational semantics of circular and non-well-founded proofs, Université Paris Diderot, started in October 2019, supervised by Thomas Ehrhard and Alexis Saurin.

- PhD started: Hugo Moeneclaey, Syntax of spheres in homotopy type theory, Université Paris Diderot, started in September 2019, supervised by Hugo Herbelin.

- PhD in progress: Antoine Allioux, Opetopes in Type Theory, Université Paris Diderot, since March 2018, supervised by Yves Guiraud and Matthieu Soseau.

- PhD in progress: Abhishek De, Proof-nets for fixed-point logics and non-well-founded proofs, Université Paris Diderot, since October 2018, supervised by Alexis Saurin.

- PhD in progress: Cédric Ho Thanh, Opetopes for higher-dimensional rewriting and koszulity, Université Paris Diderot, since September 2017, supervised by Pierre-Louis Curien and Samuel Mimram.

- PhD in progress: Lucas Massoni Sguerra, Formal verification of mechanism design, Université PSL, since January 2018, supervised by Gérard Memmi, Fabien Coehlo, and Emilio J. Gallego Arias.

- PhD in progress: Rémi Nollet, Validity conditions for circular proofs, Université Paris Diderot, since October 2016, supervised by Alexis Saurin and Christine Tasson.

- PhD in progress: Théo Winterhalter, Metatheory and certified implementation of type theories, Université de Nantes, since September 2017, supervised by Nicolas Tabareau and Matthieu Sozeau.

- PhD ended: Gaëtan Gilbert, A type theory with definitional proof-irrelevance, École Nationale Supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire - IMT Atlantique, defended on 20 December 2019, supervised by Nicolas Tabareau and Matthieu Sozeau.

- PhD ended: Théo Zimmermann, Challenges in the collaborative evolution of a proof language and its ecosystem, Université Paris Diderot, defended on 12 December 2019, supervised by Hugo Herbelin and Yann Régis-Gianas.

*9.2.2.2. Internships*

- Hugo Herbelin supervised the master internship of Adrien Champougny on a type-theoretic presentation of Primitive Recursive Arithmetic.
- Hugo Herbelin supervised the master internship of Hugo Moeneclaey on a syntax and semantics for cubical type theory with definitional univalence.
- Yann Régis-Gianas supervised the third-year licence internship of Alexandre Moine about the detection of clones in OCaml programs.
- Yann Régis-Gianas supervised the first-year master internship of Astyax Nourel and Sébastien Lecleire about the implementation of an instance server for Learn-OCaml.
- Yann Régis-Gianas cosupervised with Thomas Letan (ANSSI) the master internship of Vincent Tourneur about the certification of a Unix utility using FreeSpec.
- Alexis Saurin supervised the first-year master internship of Lucien David about Coq formalisation of circular proof systems.
- Alexis Saurin cosupervised with Benoît Valiron the MPRI internship of Kostia Chardonnet on (co)inductive types in reversible programming languages.

### 9.2.3. Juries

- Hugo Herbelin was reviewer of the PhD of Ulysse Gérard.
- Hugo Herbelin was president of the PhD committee of Kenji Maillard.
- Alexis Saurin was member of the jury of the entrance competition to Écoles normales supérieures, in charge of the computer science exam (informatique-mathématiques), for the last three years.

## 9.3. Popularisation

### 9.3.1. Internal or external Inria responsibilities

- Yves Guiraud is "correspondant communication" for IMJ-PRG at INSMI.
- Yann Régis-Gianas is "correspondant communication" for IRIF at INS2I.
- Jean-Jacques Lévy is member of the Inria-Alumni's executive committee (4 meetings in 2019).

### 9.3.2. Education

- Yann Régis-Gianas presented the Learn-OCaml project at the OCaml workshop, at the OCaml Meetup, at the University of Lisbon and at the JFLA.
- Yann Régis-Gianas gave a talk at the conference of CPGE teachers of computer science to present the Learn-OCaml project.

### 9.3.3. Interventions

- Jean-Jacques Lévy was invited by the French Academy of Sciences to participate to the Nanjing Tech Week (June 22-24) and to visit the new Qingdao International Academician Park (June 28). He also visited the Institute of Software of the Chinese Academy of Sciences (ISCAS) on July 1-3.
- Jean-Jacques Lévy as a member of the AEFC (Association des Experts France Chine) was invited to the 2019 Hangzhou International Human Resources Exchanges and Cooperation Conference (Hangzhou, November 9-11). He also visited the East China Normal University (ECNU) Shanghai (November 12-15) and Jinan University at Guangzhou (November 18-19).
- Jean-Jacques Lévy gave a talk about the Four Ages of Computer Science at the Huashang College in Guangzhou (November 18).

### 9.3.4. Internal action

Jean-Jacques Lévy talked about "L'informatique en 4 temps" at the Café des Sciences at Inria Rocquencourt (February 12) and to the Journées Européennes du Patrimoine at Inria-Rocquencourt (21 September).

<span style="color:red">**STAMP Project-Team**</span>

# 8. Dissemination

## 8.1. Promoting Scientific Activities

### 8.1.1. Scientific Events: Organisation

#### 8.1.1.1. Member of the Organizing Committees

Yves Bertot and Maxime Dénès organized the Coq User and Developer workshop in Sophia Antipolis, June 3–7, 2019.

### 8.1.2. Scientific Events: Selection

#### 8.1.2.1. Member of the Conference Program Committees

Enrico Tassi was a member of the PC for PADL and LFMTP. Benjamin Grégoire was a member of the PC for latincrypt and PriSC. Cyril Cohen was a member of the PC for CICM. Yves Bertot was a member of the PC for ITP.

#### 8.1.2.2. Reviewer

Benjamin Grégoire: Conference on Computer and Communication Security (CCS), Certified Programs and Proofs (CPP), Interactive Theorem Proving (ITP). Cyril Cohen: LICS.

### 8.1.3. Journal

#### 8.1.3.1. Reviewer - Reviewing Activities

Laurent Théry: Journal of Automated Reasoning, Science of Computer Programming, Formal Aspects of Computing. Cyril Cohen: MSCS (Journal on Mathematical Structures in Computer Science), Journal of Automated Reasoning, Theoretical Computer Science, Information Processing Letters.

### 8.1.4. Invited Talks

Enrico Tassi gave talks at the Coq developer Working Group on the migration of the package index from opam v1 to opam v2 and at the Coq workshop on the improvements to SSReflect in Coq 8.10 (with E. Martin-Dorel from the University of Toulouse). He also gave a talk in the seminar of the Inria Parsifal project-team on synthesizing proved equality tests.

Benjamin Grégoire gave an invited talk at PriSC (Principles of Secure Compilation) in January 2019.

Cyril Cohen gave a talk at the *Lean Together* meeting in 2019, on using unification hints.

### 8.1.5. Scientific Expertise

Yves Bertot is a member of the steering committee for the Inria-Nomadic Labs collaboration.

Yves Bertot is a member of the steering committee for the ITP series of conferences.

Yves Bertot was a member of the hiring committee for an associate professor at ENSIIE (Ecole Nationale Supérieure d'Informatique pour l'Industrie et l'Entreprise) in Evry, France.

### 8.1.6. Research Administration

Benjamin Grégoire is a member of the CUMI committee facilitating communication between IT services, administrative services, and researchers at Inria.

Yves Bertot was coordinator for the evaluation of the theme "Proof and verification" in March 2019. This work involved polling 13 heads of Inria project teams for names of international experts, selecting an appropriate panel, and attributing a small group of experts to each project-team.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

Master : Yves Bertot, "Proofs and reliable programming using Coq", 21hours ETD, Sept-Nov 2019, Université Nice Côte d'Azur, France.

Doctorat : Benjamin Grégoire, "EasyCrypt and Jasmin", 14 ETD, summer school on Formal Techniques, Menlo College, California, USA, 18–25 May 2019.

Doctorat : Benjamin Grégoire, "Formal verification of masked implementations" Summer school on security of software/Hardware interfaces, 3 ETD, 8–12 July 2019, Inria, France.

Doctorat : Yves Bertot "Coq introductory course", EUTypes summer school, 6 ETD, Ohrid, Aug. 30–Sep. 4, 2019, North Macedonia.

### 8.2.2. Supervision

PhD: Damien Rouhling, *Formalization Tools for Classical Analysis – A Case Study in Control Theory*, Université Côte d'Azur, September 2019, supervised by Yves Bertot and Cyril Cohen [1].

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.

Benjamin Grégoire and Tamara Rezk (Indes) supervise the doctoral thesis of Mohamad El Laz.

### 8.2.3. Juries

Yves Bertot was a member of the Jury for the Habilitation to direct research of Guillaume Melquiond.

Laurent Théry was a member of the thesis committee for David Braun (University of Strasbourg).

Laurent Théry was an external reviewer for a PhD at ANU (Australia, anonymity rules apply).

Enrico Tassi was a member of the Jury for the PhD defense of Ulysse Gérard (Inria Saclay).

Yves Bertot was a member of the Jury with report duties for the thesis of Florian Faissole (University of Paris-Saclay).

Yves Bertot was a member of the Jury with report duties for the thesis of Armaël Guéneau (University of Paris Diderot).

Yves Bertot was a member of the Jury for the thesis of Gaëtan Gilbert (Institut Mines Télécom Atlantique, Nantes).

## 8.3. Popularization

### 8.3.1. Internal action

- Yves Bertot gave a talk on Coq in the *Café-In* series of seminars for all publics of Inria personnel.
- Yves Bertot gave a general presentation on Coq in the *Doctoral seminar* of Inria Sophia Antipolis Méditerranée.

<h1 style="text-align: center; color: red;">SUMO Project-Team</h1>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

- Hervé Marchand is a member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems). He is the president of the steering committee of MSR (modélisation de systèmes réactifs).
- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the Summer School MOVEP (*Modélisation et Vérification des Processus Parallèles*).
- Blaise Genest is member of the steering comittee of the international workshop FMAI (*Formal Methods and Artificial Intelligence*).

*10.1.1.2. Member of the Organizing Committees*

- Blaise Genest coorganized the 2nd workshop FMAI 2019 (Rennes, 2-3 May 2019).

### 10.1.2. Scientific Events Selection

*10.1.2.1. Member of the Conference Program Committees*

- Éric Badouel was member of the Program Committees of VECOS, ATAED, ICTAC, CRI, and JIMIS in 2019.
- Nathalie Bertrand was a member of the Program Committees of the following international events: TIME'19, RP'19, MFCS'19.
- Éric Fabre was a member of the Program Committee of CREST'19.
- Blaise Genest was a member of the Program Committee of FMAI'19.
- Loïc Hélouët was member of the Program Committee of ACSD'2019.
- Thierry Jéron served on the Program Committees of ICTSS'19 and SAC-SVT'20.
- Nicolas Markey was a member of the Program Committee of LATA'20.
- Ocan Sankur was a member of the Program Committee of FORMATS'19.

*10.1.2.2. Reviewer*

In 2019, 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.
- Hervé Marchand is associate editor of the journal Discrete Event Dynamical Systems - Theory and applications since january 2019.

*10.1.3.2. Reviewer - Reviewing Activities*

In 2019, 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

- Nathalie Bertrand gave an invited talk at the international conference Formats'19 on Taming real-time stochastic systems.

- Blaise Genest was invited to the workshop SinFra'19 in Singapore and gave a talk on Trust in AI.

- Léo Henry was invited to a workshop on test generation by IMDEA (Madrid) to give a talk about test generation for timed automata using games.

### 10.1.5. Leadership within the Scientific Community

Nathalie Bertrand is the co-head of the *Groupe de Travail Vérif* (together with Pierre-Alain Reynier (LIS, Marseille)) which is part of *GDR Informatique Mathématique (GDR-IM)*.

### 10.1.6. Scientific Expertise

- Nathalie Bertrand was a reviewer for Thelam Fund and FWO (Belgium) and Grenoble-MSTIC. She served on the HCERES committee for Vérimag.

- Blaise Genest was reviewer for a DIGICOSME project.

- Loïc Hélouët was reviewer for ANR.

- Thierry Jéron was a reviewer for NWO (Netherlands Organisation for Scientific Research).

- Nicolas Markey served on the HCERES committee for LACL.

### 10.1.7. Research Administration

- Éric Badouel is the co-director (with Moussa Lo, UGB, Saint-Louis du Sénégal) of LIRIMA, the Inria International Lab for Africa. He is scientific officer for the African and Middle-East region at Inria DPEI (European and International Partnership Department). He is member of the executive board of GIS SARIMA.

- Nathalie Bertrand was nominated member of the Conseil National des Universités, section 27 (computer science) until November 2019.

- Emily Clément is a representative of PhD students in the Comité de Centre of Inria Rennes.

- 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 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.
  Éric Fabre is also a member of Inria Evaluation Commission since September 2019.

- Loïc Hélouët is member of Inria CNHSCT (committee for Health and Security). He is also a suppletive member in the Comité de Centre of Inria Rennes. He leads a working group of the comittee on harrassment, and another of daily life improvement. He is member of a commission at IRISA on harrassment.

- Thierry Jéron is a member of the IFIP Working Group 10.2 on Embedded Systems. He is a member of the Comité d'orientation scientifique (COS) of IRISA Rennes. He was member of the Comité de Centre of Inria Rennes until mid-2019. Since 2016 he is "référent chercheur" for the Inria-Rennes research center.

- Hervé Marchand was chairman of the *Comission des utilisateurs des moyens informatiques* (CUMI) in Rennes until December 2019. He is an elected member of the Comité de Centre at Inria Rennes since June 2019.

- Nicolas Markey manages the mentoring programme at Irisa/InriaRBA; this programme aims at having senior researchers transfering their experience to younger colleagues (including PhD students and postdoc). The programme currently concerns about 30 mentor/mentee pairs.

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Licence: Nathalie Bertrand, Advanced Algorithms (ALGO2), 20h, L3, Univ Rennes 1, France;

Licence: Loïc Hélouët, JAVA and algorithms, L2, 40h, INSA de Rennes, France.

Master: Éric Badouel, Logic and argumentation, 32h, Univ Yaoundé I, Cameroon.

Master: Nathalie Bertrand, Language Theory; Algorithms, 20h, Agrégation, ENS Rennes, France.

Master: Éric Fabre, Models and Algorithms for Distributed Systems (MADS), 10h, M2, Univ Rennes 1, France;

Master: Éric Fabre, Information Theory, 15h, M1, ENS Rennes, France.

Master: Loïc Hélouët, Algorithms, 4h, Agrégation, ENS Rennes, France;

Master: Loïc Hélouët, Algorithms and proof, 12h, Agrégation, ENS Rennes, France;

Master: Nicolas Markey, Verification of Complex Systems (CSV), 15h, M2, Univ Rennes 1, France;

Master: Nicolas Markey, Algorithms, 12h, 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;

### 10.2.2. Supervision

#### 10.2.2.1. PhD Students

- PhD: Robert Fondze Jr Nsaibirni, A Guarded Attribute Grammar Based Model for User Centered, Distributed, and Collaborative Case Management – Case of the Disease Surveillance Process [3], supervised by Éric Badouel. Defended at the University of Yaoundé I, Cameroon in April 2019.

- PhD: Karim Kecir, Performance Evaluation of Urban Rail Traffic Management Techniques [2], supervised by Loïc Hélouët and Pierre Dersin (Alstom), Université Rennes 1, July 2019.

- PhD: Samy Jaziri, Automata on Timed Structures, supervised by Nicolas Markey, Université Paris Saclay, September 2019.

- PhD: Mauricio Gonzalez, Stochastic Games on Graphs with Applications to Smart-Grids Optimization, supervised by Nicolas Markey, Université Paris Saclay, November 2019.

- PhD: Hugo Bazille, Detection and Quantification of Events in Stochastic Systems [1], supervised by Blaise Genest and Éric Fabre, Université Rennes 1, December 2019.

- PhD: The Anh Pham, Efficient state-space exploration for asynchronous distributed programs - Adapting unfolding-based dynamic partial order reduction to MPI programs [4], supervised by Thierry Jéron and Martin Quinson (Myriads, Inria Rennes), ENS Rennes, December 2019.

- 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 Clément, 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, started in September 2017, 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: Abdul Majith, Control of Adaptive Systems, started in Jan. 2019, supervised by Hervé Marchand, Ocan Sankur, and Dinh Thai-Bui (Nokia Bell Labs).
- PhD in progress: Anirban Majumdar, Games for distributed networks: models and algorithms, ENS Paris Saclay, started Sept 2018, supervised by Nathalie Bertrand and Patricia Bouyer (LSV).
- 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 and Ocan Sankur.
- PhD in progress: Rituraj Singh, Data-centric Workflows for Crowdsourcing Applications, started Feb. 2018, supervised by Loïc Hélouët.
- PhD in progress: Bastien Thomas, Automated verification of randomized distributed algorithms, started in Oct. 2019, supervised by Nathalie Bertrand and Josef Widder (Interchain, Austria).

*10.2.2.2. Master Students*

- Nathalie Bertrand supervised the master's thesis (M2) of Bastien Thomas, feb-june 2019.
- Blaise Genest and and Léo Henry supervise (2 h/week during 6 months) Alexandre Drewery, a master 1 student. The topic is reinforcement learning of mixed discrete/continuous systems.

*10.2.2.3. Other Internships*

- L3 Internship of Pierre Boudard, ENS ULM, supervised by Éric Fabre.
- L2 Internship of Kritin Garg, supervised by Éric Fabre and Blaise Genest.
- L3 Internship of Sharvik Mital, supervised by Blaise Genest and Loïc Hélouët.
- L3 Internship of Mathieu Poirier, supervised by Éric Badouel and Adrian Puerto Aubel.

### *10.2.3. Juries*

*10.2.3.1. PhD Defenses*

- Nathalie Bertrand was an examiner for the PhD thesis of Damien Busatto-Gaston (Université Aix-Marseille, december 2019).
- Éric Fabre took part to the jury for the PhD in Computer Science of Maha Mdini, Institut Mines Telecom (IMT) Atlantique, Sept. 2019
- Blaise Genest was a reviewer for the PhD of Sukanya Basu, IIT Bombay, India.
- Hervé Marchand was an examiner in the PhD defense of Raphael Jakse, Université Grenoble Alpes in December 2019.
- Nicolas Markey was a reviewer for the PhD thesis of Nicola Gigante, Jan 2019, University Udine, Italy.

*10.2.3.2. Other Juries*

- Nathalie Bertrand was in the *Moyens incitatifs* committee for Inria Rennes Bretagne Atlantique in 2019.
- Éric Fabre was in the hiring committee for CRCN positions at Inria Rennes Bretagne Atlantique in 2019.
- Ocan Sankur was in the hiring committee for two Maitre de conférences positions at Université de Nantes in 2019.

## 10.3. Popularization

### *10.3.1. Education*

Nicolas Markey is involved in the organization of action "J'Peux Pas, J'Ai Informatique", whose aim is to break down stereotypes about computer science for 12-year-old pupils.

# TOCCATA Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

J.-C. Filliâtre, scientific chair and co-organizer of EJCP (École Jeunes Chercheurs en Programmation du GDR GPL) at Strasbourg on June 24–28, 2019. 5 days / 8 lectures / 25 participants. http://ejcp2019.icube.unistra.fr/

### 10.1.2. Scientific Events: Selection

*10.1.2.1. Chair of Conference Program Committees*

S. Boldo, program co-chair of the 26th IEEE Symposium on Computer Arithmetic (ARITH 2019), Kyoto, Japan. [35]

*10.1.2.2. Member of the Conference Program Committees*

S. Boldo, 11th NASA Formal Methods Symposium (NFM 2019)

J.-C. Filliâtre, 10th International Conference on Interactive Theorem Proving (ITP 2019)

J.-C. Filliâtre, 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)

J.-C. Filliâtre, European Symposium on Programming (ESOP 2020)

G. Melquiond, 26th IEEE Symposium on Computer Arithmetic (ARITH 2019)

G. Melquiond, 10th International Conference on Interactive Theorem Proving (ITP 2019)

*10.1.2.3. Reviewer*

The members of the Toccata team have reviewed numerous 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

G. Melquiond, "Computer Arithmetic and Formal Proofs" [19], at the 30th Journées Francophones des Langages Applicatifs (JFLA 2019).

J.-C. Filliâtre, "Deductive Verification of OCaml Libraries" [17], at the 15th International Conference on integrated Formal Methods (iFM), December 2019, Bergen, Norway.

J.-C. Filliâtre, "Retour sur 25 ans de programmation avec OCaml" [18], at Journées Francophones des Langages Applicatifs (JFLA), January 2019, Les Rousses, France.

J.-C. Filliâtre, "The Why3 tool for deductive verification and verified OCaml libraries", at Frama-C/Spark day 2019, Paris, France.

### 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) and now L.-S. Didier (Univ. Toulon).

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").

S. Boldo, member of the program committee for selecting postdocs of the maths/computer science program of the Labex mathématique Hadamard.

S. Boldo has mentored for 1 year a female PhD student of University Paris-Saclay (from epidemiology).

J.-C. Filliâtre, grading the entrance examination at X/ENS (*"option informatique"*).

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 (national) IES commission.

S. Boldo, member of the CDT commission of Saclay (*"commission de développement technologique"*).

S. Boldo, member of the STIC department commission of Univ. Paris-Sud.

S. Boldo, member of the executive commission for the Digicosme Labex.

S. Boldo, deputy scientific director (DSA) of Inria Saclay research center from January 1st, 2019

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

Master Parisien de Recherche en Informatique (MPRI) https://wikimpri.dptinfo.ens-cachan.fr/doku.php: "Proofs of Programs" http://www.lri.fr/~marche/MPRI-2-36-1/ (M2), C. Marché (12h).

A. Lanco, *Unix et programmation Web*, 24h, L2, Université Paris-Saclay, France.

G. Melquiond, *Programmation C++ avancée*, 12h, M2, Université Paris-Saclay, France.

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.

S. Boldo was invited in the Xavier Leroy's course at Collège de France on Dec 19th.

### 10.2.2. Supervision

HDR: G. Melquiond, "Formal Verification for Numerical Computations, and the Other Way Around" [11], Université Paris-Sud, Apr. 1st, 2019.

PhD: F. Faissole, "Formalisations d'analyses d'erreurs en analyse numérique et en arithmétique à virgule flottante", Université Paris-Saclay & Université Paris-Sud, Dec 13th 2019, supervised by S. Boldo and A. Chapoutot. [Not yet on HAL]

PhD: A. Coquereau, "Amélioration de performances du solveur SMT Alt-Ergo grâce à l'intégration d'un solveur SAT efficace", Université Paris-Saclay & Université Paris-Sud, Dec 16th 2019, supervised by S. Conchon, F. Le Fessant et M. Mauny. [Not yet on HAL]

PhD: M. Roux, "Extensions de l'algorithme d'atteignabilité arrière dans le cadre de la vérification de modèles modulo théories", Université Paris-Saclay & Université Paris-Sud, Dec 19th 2019, supervised by Sylvain Conchon. [Not yet on HAL]

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.

PhD in progress: A. Lanco, "Stratégies pour la réduction forte", since Oct. 2019, supervised by T. Balabonski and G. Melquiond.

G. Turbiau has been a M1 trainee for 2 months, supervised by S. Boldo.

### 10.2.3. Juries

S. Boldo, member of the Inria CRCN recruiting juries, national one and at Rennes.

S. Boldo, president of the PhD defense of Clothilde Jeangoudoux, Sorbonne University, May 21st

S. Boldo, reviewer of the habilitation of Christoph Lauter, Sorbonne University, May 22nd

S. Boldo, reviewer of the PhD defence of Florent Bréhard, ENS Lyon, July 12th

S. Boldo, reviewer of PhD defence of Damien Rouhling, Université Côte d'Azur, Sept 30th

S. Boldo, president of the PhD defense of Yohan Chatelain, Université Paris-Saclay, Dec 12th

S. Boldo, president of the PhD defense of Armaël Guéneau, Université de Paris, Dec 16th

S. Boldo, member of the PhD defense of Antoine Kaszczyc, Université Paris-Nord, Dec 18th

J.-C. Filliâtre, reviewer of the PhD defense of Y. El Bakouny, "Scallina: On the Intersection of Scala and Gallina", Université Saint-Joseph, Beirut, Lebanon, December 19, 2019.

J.-C. Filliâtre, president of the PhD defense of L. Blatter "Relational properties for specification and verification of C programs in Frama-C", University Paris Saclay, September 26, 2019.

## 10.3. Popularization

### 10.3.1. Internal or external Inria responsibilities

S. Boldo has been the scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria until October 2019.

She was also responsible (with A. Couvreur of the Grace team a,d M. Quet of the SCM) for the 2019 "Fête de la science" on October 10th and 11th 2019. 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. Education

S. Conchon and J.-C. Filliâtre, together with K. Nguyen and T. Balabonski (members of the LRI team but not members of Toccata), wrote a book "Numérique et Sciences Informatiques, 30 leçons avec exercices corrigés" (Ellipses, August 2019) [36] targeting the new Computer Science programme in the French high school system, which started in September 2019.

S. Boldo gave a talk and was involved in the organization of the "Rencontres des Jeunes mathé-maticiennes et Informaticiennes" organized in Saclay on Oct 21st and 22nd 2019. About 20 female teenagers were welcomed for two days with talks and exercises to discover research.

### 10.3.3. Interventions

C. Marché presented an overview of the Why3 tool and its ecosystem at the Paris Open Source Summit in Saint-Denis, Dec. 11, 2019, as part of a workshop "ATELIER Inria : OCaml, Coq, Why 3: pour concevoir codes et infrastructures plus sûrs en C, Java, Javascript, Ada" https://www.opensourcesummit.paris/conferences.html?date=1576022400).

S. Boldo gave a talk at a high school in Sceaux on Feb 8th.

S. Boldo presented the floating-point arithmetic at IRIF to the members of the CODYS ANR on April 1st.

<h1 style="text-align:center;color:red">VERIDIS Project-Team</h1>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Organization of Scientific Events

#### 10.1.1.1. Membership in Organizing Committees

Jasmin Blanchette co-organized the *2nd Deduction Mentoring Workshop* (DeMent 2019). He also coorganized the *VeriDis Group Retreat + Second European Workshop on Higher-Order Automated Reasoning* (Matryoshka 2019).

Pascal Fontaine co-organized the Third Workshop on Mathematical Logic and its Applications, in Nancy.

Igor Konnov and Stephan Merz were organizers of the sixth *Workshop on Formal Reasoning in Distributed Algorithms* (FRIDA 2019), colocated with DISC 2019 in Budapest, Hungary.

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 2019, VTSA took place in August in Esch sur Alzette, Luxembourg.

### 10.1.2. Program Committees

#### 10.1.2.1. Chair of Conference Program Committees

Jasmin Blanchette co-chaired the program committee of the *9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (CPP 2020).

Pascal Fontaine served as the chair of the *Conference on Automated Deduction* (CADE-27).

Dominique Méry co-chaired the program committee of the *13th International Symposium on Theoretical Aspects of Software Engineering* (TASE 2019).

Stephan Merz was Tool Exhibition Chair at the *3rd World Congress for Formal Methods* (FM Week 2019).

#### 10.1.2.2. Membership in Conference Program Committees

Jasmin Blanchette served on the program committees of the *27th International Conference on Automated Deduction* (CADE-27), *19th Conference on Formal Methods in Computer-Aided Design* (FM-CAD 2019), *21st International Symposium on Principles and Practice of Declarative Programming* (PPDP 2019), *12th International Symposium on Frontiers of Combining Systems* (FroCoS 2019), *26th International Conference on Tools and Algorithms for the Construction and Analysis of Systems* (TACAS 2020), and *4th Conference on Artificial Intelligence and Theorem Proving* (AITP 2019). He also served on the following workshop committees: *Second Workshop on Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2019) and *Deduktionstreffen 2019*.

Pascal Fontaine served on the program committees of the *International Symposium on Frontiers of Combining Systems* (FroCoS 2019), the *International Conference on Automated Reasoning with Analytic Tableaux and Related Methods* (TABLEAUX 2019), and the *International Conference on Theory and Applications of Satisfiability Testing* (SAT 2019). He also served on the committee of *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2019).

Dominique Méry served on the program committees of the *16th International Colloquium on Theoretical Aspects of Computing* (ICTAC 2019), the *8th Workshop on Formal Methods for Interactive Systems* (FMIS 2019), the *Workshop on Practical Formal Verification for Software Dependability* (AFFORD'19), the *24th International Conference on Engineering of Complex Computer Systems* (ICECCS 2019), the *Workshop on Formal Methods for Autonomous Systems* (FMAS 2019), the *23rd International Symposium on Formal Methods* (FM 2019), the *Workshop on Models and Data Engineering for Cyber-Physical Systems* (CPS@MEDI 2019), the *Workshop on Formal Models for Mastering Heterogeneous Multifaceted Systems* (REMEDY 2019), the *3rd Workshop on Formal Approaches for Advanced Computing Systems* (FAACS 2019), the *21st International Conference on Formal Engineering Methods* (ICFEM 2019), and the *9th International Conference on Model and Data Engineering* (MEDI 2019).

Stephan Merz served on the program committees of the *19th International Workshop on Automated Verification of Critical Systems* (AVoCS 2019), the *Doctoral Symposium, Formal Methods* (DS-FM 2019), the *5th International Workshop on Formal Integrated Development Environment* (F-IDE 2019), and the *21st International Conference on Formal Engineering Methods* (ICFEM 2019).

Sorin Stratulat served on the program committees of the *International Symposium on Symbolic and Numeric Algorithms for Scientific Computing* (SYNASC 2019), the *International Conference on Information Assurance and Security* (IAS 2019), and the *International Conference on Computational Intelligence in Security for Information Systems* (CISIS 2019).

Thomas Sturm served on the program committees of the *21st International Workshop on Computer Algebra in Scientific Computing* (CASC 2019) and the *4th International Workshop on Satisfiability Checking and Symbolic Computation* (SC-SQUARE 2019).

Uwe Waldmann served on the program committees of the *27th International Conference on Automated Deduction* (CADE-27) and the *International Conference on Automated Reasoning with Analytic Tableaux and Related Methods* (TABLEAUX 2019).

Christoph Weidenbach served on the program committees of the *International Conference on Automated Deduction* (CADE 27), and the *International Symposium on Frontiers of Combining Systems* (FroCoS 2019). He also served on the committee of *Automated Reasoning: Challenges, Applications, Directions, Exemplary Achievements* (ARCADE 2019).

## 10.1.3. Journals

### 10.1.3.1. 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* [16].

Dominique Méry is the Book Reviews Editor for *Formal Aspects of Computing*.

Thomas Sturm has been an editor of the *Journal of Symbolic Computation* (Elsevier) since 2003 and an editor of *Mathematics in Computer Science* (Springer) since 2013. He edited a special issue of the Journal of Symbolic Computation on *Symbolic Computation and Satisfiability Checking*.

Christoph Weidenbach is a member of the editorial board of the *Journal of Automated Reasoning* (JAR) (Springer). He also served as an editor on the special issue on *Automated Reasoning Systems* of JAR.

## 10.1.4. Invited Talks

Jasmin Blanchette gave a keynote talk at the *8th ACM SIGPLAN International Conference on Certified Programs and Proofs* (CPP 2019).

Dominique Méry was an invited speaker at the *16th International Colloquium on Theoretical Aspects of Computing* (ICTAC 2019).

Stephan Merz was invited to the meeting of IFIP Working Group 2.3 in October 2019 in Los Altos, California. He was an invited speaker at the meeting of the AFSEC group of GDR GPL in December 2019 in Toulouse.

Sorin Stratulat was an invited speaker at FROM 2019 (Working Formal Methods Symposium) in Timisoara, Romania, where he presented an efficient way to validate cyclic pre-proofs for first-order logic with inductive definitions.

Christoph Weidenbach was invited to give a lecture at the SAT/SMT/AR summer school 2019 in Lisbon, Portugal. He was invited to present at the computer science lecture series at the University of Bonn, Germany.

### 10.1.5. Leadership within the Scientific Community

Jasmin Blanchette served as 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.

Pascal Fontaine is an SMT-LIB manager, together with Clark Barrett (Stanford University) and Cesare Tinelli (University of Iowa). He was a regular member of the steering committee for the FroCoS (*Frontiers of Combining Systems*) conference series until September 2019, and he is a member of the steering committee for the SC-Square (*Satisfiability Checking and Symbolic Computation* workshop series. He was ex-officio member of the CADE (*Conference on Automated Deduction*) Inc. Board of Trustees until July 2019. 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* and a member of the steering committee of the workshop on Automated Verification of Critical Systems (AVoCS).

Thomas Sturm has been elected the chair 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.

### 10.1.6. Scientific Expertise

Dominique Méry was a member of the committee for the thesis award of GDR GPL (*Génie de la Programmation et du Logiciel*) 2019.

Stephan Merz contributed an assessment of candidates for a professorship at TU Vienna, Austria.

Thomas Sturm served as an external expert on the appointment committee for a professorship in Computer Algebra at the University of Kassel, Germany. He is taking an advisory role as a "project partner" in the UK EPSRC Project EP/R019622/1 *Embedding Machine Learning within Quantifier Elimination Procedures*.

Christoph Weidenbach is a member of the selection committee of the Saarbrücken Graduate School in Computer Science.

### 10.1.7. Research Administration

Dominique Méry participated in the evaluation committees of HCERES for the LIASD (*Laboratoire d'informatique avancée de Saint-Denis*) and the doctoral school of École Polytechnique.

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 2019, he was a member of the hiring committees of senior researchers at Inria and of junior researchers at Inria Rennes Bretagne Atlantique. 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 coordinates the scientific affairs at MPI-INF.

# 10.2. Teaching, Supervision, Thesis Committees

## 10.2.1. Teaching

Licence : Marie Duflot-Kremer, Algorithmique et Programmation 1, 60 HETD, L1, Université de Lorraine, France

Licence : Marie Duflot-Kremer, Algorithmique et Programmation 2, 10 HETD, L1, Université de Lorraine, France

Diplôme inter universitaire : Marie Duflot-Kremer, formation d'enseignants du secondaire à la spécialité NSI, 43 HETD, Université de Lorraine, France

Licence : Marie Duflot-Kremer, Introduction au Web, 20 HETD, L1, Université de Lorraine, France

Licence : Marie Duflot-Kremer, Accompagnement Algorithmique 1, 26 HETD, L1, Université de Lorraine, France

Licence : Marie Duflot-Kremer, Programmation Web, 5 HETD, L3, 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, Algorithmes distribués, 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.

Licence : Sorin Stratulat, Algorithmique des structures de contrôle, 45 HETD, L1 Informatique, ISFATES, Université de Lorraine, France.

Licence : Sorin Stratulat, Algorithmique des structures de données, 45 HETD, L1 Informatique, ISFATES, Université de Lorraine, France.

Master: Sorin Stratulat, Analyse et conception de logiciels, 105.5 HETD, M1 Informatique, Université de Lorraine, France.

Master: Sorin Stratulat, Génie Logiciel, 20 HETD, M2 Informatique, Université de Lorraine, France.

Master: Sophie Tourret, Concrete Semantics with Isabelle/HOL, 6 ECTS, Saarland University, Germany.

Master: Uwe Waldmann, Automated Reasoning, 9 ECTS, Saarland University, Germany.

Master: Christoph Weidenbach, Decision Procedures, 6 ECTS, Saarland University, Germany.

## 10.2.2. Supervision

PhD: Martin Bromberger, Decision Procedures for Linear Arithmetic. Saarland University, 10 December 2019. Supervised by Thomas Sturm and Christoph Weidenbach.

PhD: Nicolas Schnepf, Orchestration et vérification de fonctions de sécurité pour des environnements intelligents. Université de Lorraine, 30 September 2019. Supervised by Rémi Badonnel, Abdelkader Lahmadi, and Stephan Merz.

PhD: Marco Voigt, Decidable Fragments of First-Order Logic and of First-Order Linear Arithmetic with Uninterpreted Predicates. Saarland University, 31 July 2019. Supervised by Thomas Sturm and Christoph Weidenbach.

PhD in progress: Antoine Defourné, SMT for TLAPS, Université de Lorraine. Supervised by Jasmin Blanchette, Pascal Fontaine, and Stephan Merz, since March 2019.

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: Alberto Fiori, Clause Learning from Simple Models, Saarland University. Supervised by Christoph Weidenbach, since August 2018.

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: Daniel El Ouraoui, Higher-Order SMT, Université de Lorraine. Supervised by Jasmin Blanchette, Pascal Fontaine, and Stephan Merz, since November 2017.

PhD in progress: Pierre Lermusiaux, Analysis of properties of interactive critical systems, Université de Lorraine. Supervised by Horatiu Cirstea and Pierre-Etienne Moreau, since October 2017.

PhD in progress: Hans-Jörg Schurr, Higher-Order SMT, Université de Lorraine. Supervised by Jasmin Blanchette, Pascal Fontaine, and Stephan Merz, since November 2017.

### 10.2.3. Thesis Committees

Pascal Fontaine served as a reviewer in the thesis committees for Martin Bromberger (Universität des Saarlandes, Germany), Albin Coquereau (Université Paris-Saclay, France), Hakan Metin (Sorbonne Université, France), Simon Robillard (Chalmers University of Technology, Sweden) and Stefano Varotti (University of Trento, Italy).

Stephan Merz served as an examiner in the PhD committee of The Anh Pham (ENS Rennes) and as the president in the PhD committee of Renaud Vilmart (Univ. of Lorraine). He was a member of the PhD committee of Nicolas Schnepf as the thesis advisor.

Thomas Sturm served as a reviewer in the thesis committees for Martin Bromberger and Marco Voigt (Saarland University, Germany).

Christoph Weidenbach served as a reviewer in the thesis committees for Martin Bromberger and Marco Voigt (Saarland University, Germany).

## 10.3. Popularization

### 10.3.1. Responsibilities at Inria or Beyond

- Marie Duflot-Kremer is the deputy vice-president for outreach activities in the supervisory council of SIF (*Société Informatique de France*) and a member of the scientific committee of *Fondation Blaise Pascal*.

- Christoph Weidenbach is a member of the advisory committee for the German computer science competitions for pupils. Together with his colleagues at Saarland university he organizes the "Computer Science Research Days" for the most talented high-school students out of the competition every year. In addition, he organizes the final training for the German Informatics Olympiad team and coaches the Saarland University student teams for the ICPC.

### 10.3.2. Articles and Contents

Marie Duflot-Kremer is a member of the ERASMUS+ project PIAF (cf. section 9.3 ) with collleagues from Liège, Luxembourg and Saarbrücken. This projects aims at studying how computational thinking can be introduced in primary education (with kids rangng from 5 to 12 years old). The goal is first to agree on a shared reference document on computational thinking competences, and then to produce and test educational scenarios and didactical resources. So far this year the reference document has been designed (and a paper has been submitted recently to a conference). The work on the scenarios and the resources is ongoing.

### 10.3.3. Education

Marie Duflot-Kremer intervenes in the training of teachers:

- for primary school, half a day for training teachers on how to add a bit of computer science in their teaching;
- for secondary school, she took part (43 hours in 2019) in the advanced training of high school teachers who deliver a newly introduced computer science course (Numérique et Sciences Informatiques), and one day training for math teachers about unplugged activities;
- half a day of training for members of INSPE (Institut National Supérieur du Professorat et de l'Education), the people in charge of training teachers.

### 10.3.4. Interventions

Marie Duflot-Kremer takes part every year in several events, including local ones such as *Fête de la Science* (for which she trains 3rd year students to handle the workshops and gave this year a talk/show on "informagics"), Pint of Science, a talk for the local phase of the *Tournoi Français des Jeunes Mathématiciennes et Mathématiciens* and the local NSI (*Numérique et Sciences Informatiques*) day for secondary school teachers.

She is also invited for workshops and talks in events outside of the Nancy region, like national or regional days of APMEP (*Association des Professeurs de Mathématiques de l'Enseignement Public*) in Dijon and Grenoble, the SETT conference in Namur or the video game creation competition for kids in Manosque.

### 10.3.5. Creation of Media or Tools for Science Outreach

As a member of the national group *Informatique Sans Ordinateur* (ISO), Marie Duflot-Kremer takes part in creating new popularization activities and publishing online documentation to help people reproduce unplugged computer science activities. She also proposed and supervised a project of master students in cognitive sciences who created an escape game presenting various computer science concepts to kids from 13 years old. The documentation is available on her webpage. [0]

---

[0]https://members.loria.fr/MDuflot/.

<h1 style="text-align:center; color:red">CIDRE Project-Team</h1>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Organisation

#### 9.1.1.1. General Chair, Scientific Chair

- Ludovic Mé served as general chair of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.
- Guillaume Hiet is the chair holder of the SILM thematic semester. He served as general chair of the SILM workshop, November 2019, Rennes, France.

The SILM thematic semester [0] is dedicated to the security of software/hardware interfaces and focus more particularly on the three following axes:

1. Analyzing the behavior and the state of hardware components using, e.g. trace mechanisms, fuzzing, reverse-engineering techniques, or side channel analyses;

2. Studying the hardware vulnerabilities and the software attacks that can exploit them: e.g. side-channels, fault injections, or exploitation of unspecified behavior;

3. Detecting and preventing software attacks using dedicated hardware components. Proposing software countermeasures to protect from hardware vulnerabilities.

The goal of this semester is to promote the scientific, teaching and industrial transfer activities on the security of software/hardware interfaces. Our objective is also to identify scientific and technological challenges in that field and to propose a strategic action plan. To that end, we organized different events:

- The SILM summer school (in collaboration with the GDR "Sécurité Informatique") [0], in July 2019, Rennes, France.
- The SILM workshop [0], in Novembre 2019, Rennes, France
- A regular seminar [0] at Inria, Rennes, France.

We will also animate a working group and publish a white-paper on that topic.

#### 9.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2019 (26rd Computers & Electronics Security Applications Rendez-vous), November 2019, Rennes, France.

Eric Totel served as a member of the organization committee of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.

Gilles Guette served as a member of the organization committee of the conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information), May 2019, Erquy, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2019 (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.

---

[0] https://silm.inria.fr/
[0] https://silm-school.inria.fr/
[0] https://silm-workshop.inria.fr/
[0] https://semestres-cyber.inria.fr/en/silm-seminar/

Frédéric served as a member of the organisation committee of SILM Summer School and SILM workshop.

### 9.1.2. Scientific Events: Selection

#### 9.1.2.1. Chair of Conference Program Committees

Jean-François Lalande was the program co-chair of HPCS 2019 (The 2019 International Conference on High Performance Computing & Simulation), July 2019, Dublin, Ireland, IEEE Computer Society.

Jean-François Lalande was the program co-chair of CECC 2019 (Central European Cybersecurity Conference), November 2019, Munich, Germany, ACM Press.

Jean-François Lalande was the program co-chair of IWSMR 2019 workshop (1st International Workshop on Information Security Methodology and Replication Studies), August 2019, Dublin, Ireland, ACM Press.

#### 9.1.2.2. Member of the Conference Program Committees

Ludovic Mé served the Scientific Committee of the FIC 2020.

Frédéric Tronel and Valérie Viet Triem Tong served as a member of the program committee of SSTIC 2019 (Symposium sur la sécurité des technologies de l'information et des communications) June 2019, Rennes, France.

Jean-François Lalande served as a member of the program committee of the international conferences CECC 2019, SecITC 2019, and of international workshops IWCC 2019, CUING 2019, SHPCS 2019, WTMC 2019.

Gilles Guette served as a member of the program committee of the international conferences ICISSP 2019, ISNCC 2019, ITSC 2019.

Guillaume Piolle served as a member of the program committee of the APVP 2019 workshop.

Emmanuelle Anceaume served as a member of the program committee of NCA 2019, EDCC 2019, ICDCS 2019, DEBS 2019, TrustCom 2019, BSCT 2019 and Tokenomics 2019.

### 9.1.3. Journal

#### 9.1.3.1. Member of the Editorial Boards

Michel Hurfin serves as a member of the editorial board of the JISA Journal (Journal of Internet Services and Applications - Springer).

Jean-François Lalande served as a member of the program committee of the IARIA International Journal on Advances in Security.

#### 9.1.3.2. Reviewer - Reviewing Activities

Michel Hurfin served as a reviewer for the International Journal of Control , the Journal on Discrete Event Dynamic Systems - Theory and Applications, and IEEE Transactions on Dependable and Secure Computing.

Jean-François Lalande served as a reviewer for the following international journals: Journal of Cyber Security and Mobility, IEEE Transactions on Reliability, Journal Elsevier FGCS, IEEE Transactions on Industrial Informatics, MDPI Applied Sciences, Journal of Universal Computer Science.

Eric Totel served as a reviewer for the European Congress of Embedded Real Time Software and Systems.

Pierre Wilke served as a reviewer for the 12th International Conference on Security for Information Technology and Communications (SecITC 2019).

Guillaume Hiet served as a reviewer for the Journal of Computer Security and IEEE Design & Test

### 9.1.4. Invited Talks

Ludovic Mé. *Cyber security: current challenges*. LIRIMA Franco-African webinar. Sept. 2019.

Jean-François Lalande: *Obfuscated Android Application Development*, CECC 2019, Munich.

Emmanuelle Anceaume: *Abstractions for permissionless distributed systems*, SSL seminar, Nancy, 5 December 2019.

Emmanuelle Anceaume: *Can we safely adapt the construction of permissionless blockchains to user demand ?*, *Journées Futur & Rupture*, ParisTech, 31 March 2019.

Emmanuelle Anceaume: *Beyond the block: a lego blockumentary*, SecDays, 9-10 January 2019.

Emmanuelle Anceaume: *Round table at the "Future & Rupture day"* with Mr Ronan Le Gleut (Sénateur), Mr. Gérard Memmi (Télécom ParisTech), Mr. Nicolas KozaKiewicz (Atos Worldline) - moderator Patrick Duvaut, February, 28 2019.

### 9.1.5. Scientific Expertise

- Ludovic Mé served the HCERES evaluation committee of the LAAS-CNRS research lab.

- Ludovic Mé has served the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).

- Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR).

- Jean-François Lalande is part of the advisory board of the starting european project "SIMARGL" (H2020 project): Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware.

### 9.1.6. Research Administration

- Christophe Bidan was a member of a recruitment committee for an assistant professor position at CentraleSupélec, Rennes.

- Ludovic Mé is deputy scientific director of Inria, in charge of the cyber security domain.

- Valérie Viet Triem Tong was a member of 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 IMT, Brest.

## 9.2. Teaching - Supervision - Juries

### 9.2.1. Teaching

Team members are involved in initial and continuing education in CentraleSupélec, a french institute of research and higher education in engineering and science and ESIR (Ecole Supérieure d'Ingénieur de Rennes) the graduate engineering school of the University of Rennes 1.

In these institutions,

- Gilles Guette is director of corporate relations at ESIR;

- Jean-François Lalande is responsible of the major program dedicated to information systems security and the special track Infosec of CentraleSupélec ;

- Frédéric Tronel and Valérie Viet Triem Tong share the responsability of the *mastère spécialisé* (post-graduate specialization degree) in Cybersecurity. This education was awarded **best French master degree** in the category "Master Cybersecurity masters and Security of systems" in the Eduniversal master ranking 2019.

The teaching duties are summed up in table 1 .

| | Licence level | Master level | CS† | Univ. Rennes 1 | Initial education | Continuing education | 2018-2019 |
|---|---|---|---|---|---|---|---|
| Emmanuelle Anceaume | | ✓ | | ✓ | ✓ | | 10 |
| Christophe Bidan | ✓ | ✓ | ✓ | | ✓ | ✓ | 64 |
| Gilles Guette | ✓ | ✓ | ✓ | ✓ | ✓ | | 400 |
| Guillaume Hiet | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 328 +34* |
| Jean-François Lalande | ✓ | ✓ | ✓ | | ✓ | ✓ | 326 +70* |
| Guillaume Piolle | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 210 |
| Frédéric Tronel | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 287 |
| Valérie Viet Triem Tong | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 229 |
| Pierre Wilke | ✓ | ✓ | ✓ | | ✓ | ✓ | 140 |

*Figure 1.*

## 9.2.2. Supervision

HdR defended in 2019, Emmanuelle Anceaume, *Abstractions for permissionless systems*.

PhD defended in 2019: Aurélien Dupin, *Secure multi-partie computations*, started February 2016, supervised by Christophe Bidan(40%), David Pointcheval (30% - ENS) and Renaud Dubois (30% - Thales).

PhD defended in 2019: Aurélien Palisse, *Analyse et détection de logiciels de rançon*, started in 2015, supervised by Jean-Louis Lanet, Colas Le Guernic (DGA) and Hélène Le Bouder (IMT Atlantique);

PhD defended in 2019: 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 defended in 2019: Pernelle Mensah, *Generation and Dynamic Update of Attack Graphs in Cloud Providers Infrastructures*, started in January 2016, supervised by Eric Totel (25%), Guillaume Piolle (25%), Christine Morin (25% - Myriads Inria project), and Samuel Dubus (25% - Nokia);

PhD defended in 2019: Kevin Bukasa, *Vulnerability analysis of embedded systems against physical attacks* , supervised by Jean-Louis Lanet and Ronan Lashermes (SED Inria);

PhD defended in 2019: Ronny Chevalier, *Detecting and Surviving Intrusions - Exploring New Host-Based Intrusion Detection, Recovery, and Response Approaches*, supervised by Guillaume Hiet (50%), David Plaquin (25% - HP) and Ludovic Mé (25%);

PhD in progress: Alexandre Dey, *Continuous Model Learning for Anomaly Detection In the Presence of Highly Adaptative Cyberattacks*, started in November 2019, supervised by Eric Totel (50%) and Ludovic Mé (50%);

PhD in progress: 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: 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: 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: 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: 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%);

PhD in progress: Tomas Conception Miranda, *Profiling and Visualization Android malware*, started in October 2019, supervised by Jean-François Lalande (34%), Valérie Viet Triem Tong (33%), Pierre Wilke (33%).

*9.2.2.1. Supervision of external PhD candidates*

PhD in progress: Nicolas Bellec, *Security enhancement in embedded hard real-time systems*, started in October 2019, supervised by Isabelle Puaut (50%), Guillaume Hiet (25%), Frédéric Tronel (25%)

PhD in progress: Kevin Le Bon, *Security enhancement in embedded hard real-time systems*, started in October 2018, supervised by Erven Rohu (30%), Guillaume Hiet (35%), Frédéric Tronel (35%)

### 9.2.3. Juries

Ludovic Mé was a member of the PhD committee for the following PhD thesis:

Amina Saadaoui, *Formal Techniques for Automatic Detection and Resolution of Security Equipment Misconfigurations*, supervised by Adel Bouhoula and Sihem Guemara, University of Carthage, April 2019.

Amir Wonjiga, *User-Centric Security Monitoring in Cloud Environments*, supervised by Christine Morin and Louis Rilling, University of Rennes 1, May 2019.

Ludovic Mé was a member of the committee for the following HDR defense:

Stephane Mocanu, *Cyberdéfense des infrastructures critiques*, University Grenoble Alpes community, January 2019.

Nizar Kheir, *From Cyber-secure to Cyber-resilient Computer Systems: The way forward*, University of Paris-Saclay, May 2019.

Valérie Viet Triem Tong was a member of the PhD committee for the following PhD thesis:

Xin Ye Model, *Checking Self Modifying Code*, supervised by Tayssir Touili et Jifeng He, University of Paris, Septembre 2019.

Alexandre Dang, *Compilation Sécurisée pour la Protection de la Mémoire*, supervised by Frédéric Besson and Thomas Jensen, University of Rennes 1, December 2019.

Jean-François Lalande was a member of the PhD committee for the following PhD thesis:

M. Guillaume Averlant, *Contrôle d'accès dynamique et architecture de sécurité pour la protection des applications sous Android*, Université Fédérale Toulouse Midi- Pyrénées, october 2th 2019.

## 9.3. Popularization

### 9.3.1. Articles and contents

- In books/journals for the general public

  *Dis, c'est quoi là haut dans le ciel ? C'est un Linux, mon petit !*[39], Viet Triem Tong Valérie, Fournier Benoît, Fournier Guillaume, Ouairy Leopold, Cotret Pascal, Guette Gilles, MISC numéro 104, juillet 2019.

- Online publications

  La cybersécurité aux multiples facettes. Steve Kremer, Ludovic Mé, Didier Rémy et Vincent Roca. Blog binaire (https://www.lemonde.fr/blog/binaire/), 4 juillet 2019.

- White Papers - white Papers for Popularization

  Ludovic Mé co-authored (with S. Kremer, D. Rémy and V. Roca) Inria's White Book on Cybersecurity [37].

### 9.3.2. Interventions

- Valérie Viet Triem Tong has participated to the *Vive la Recherche* event to promote research activities to engineering students at CentraleSupelec

- Valérie Viet Triem Tong has been involved in an artistic performances involving actors and researcher at the Digital Tech Conference, December Rennes, France.

## COMETE Project-Team

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific events organisation

*9.1.1.1. Member of the organizing committee*

Catuscia Palamidessi is member of:

The Scientific Advisory Board of ANSSI, the French National Cybersecurity Agency. Since 2019.

The Scientific Advisory Board of CISPA, the Helmholtz Center for Information Security. Since 2019.

The Executive Committee of SIGLOG, the ACM Special Interest Group on Logic and Computation. 2014-19.

The Steering Committee of CONCUR, the International Conference in Concurrency Theory. Since 2016.

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.

### 9.1.2. Scientific events selection committee

*9.1.2.1. Chair of conference program committee*

Konstantinos Chatzikokolakis:

is serving as PC chair (with Carmela Troncoso as co-chair) of PETS 2020: The 20th Privacy Enhancing Technologies Symposium, July 14 – 18, 2020 Montréal, Canada.

*9.1.2.2. Member of conference program committees*

Catuscia Palamidessi is/has been a member of the program committees of the following conferences and workshops:

CCS 2020. The ACM Conference on Computer and Communications Security. Orlando, USA, November 9-13 2020.

CSF 2020. The 33rd IEEE Computer Security Foundations Symposium. Boston, MA, USA, June 22-26, 2020.

PETS 2020. The 20th Privacy Enhancing Technologies Symposium. Montréal, Canada, July 14 – 18, 2020.

FORTE 2020. The 40th IFIP International Conference on Formal Techniques for Distributed Objects, Components, and Systems. University of Malta, Valletta, June 15-19, 2020.

FSTTCS 2019. 39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science. Indian Institute of Technology Bombay, December 11–13, 2019

FACS 2019. The 16th International Conference on Formal Aspects of Component Software. Amsterdam, The Netherlands, 23-25 October 2019.

PETS 2019. The 19th Privacy Enhancing Technologies Symposium. Stockholm, Sweden, July 16 – 20, 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.

TML 2020. Towards Trustworthy ML: Rethinking Security and Privacy for ML. Addis Ababa, Ethiopia, April 26, 2020.

EXPRESS/SOS 2020. Combined 27th International Workshop on Expressiveness in Concurrency and 17th Workshop on Structural Operational Semantics. Vienna, Austria, August 31, 2020.

PPAI 2020. The rAAI Workshop on Privacy-Preserving Artificial Intelligence. New York, USA, February 7, 2020.

PPML 2019. Privacy Preserving Machine Learning (ACM CCS 2019 Workshop). London, UK, November 15, 2019.

WPES 2019. Workshop on Privacy in the Electronic Society. London, UK, November 11, 2019.

APVP 2019. Atelier sur la Protection de la Vie Privée. Cap Hornu, France, July 9-11, 2019.

WIL 2019. 3rd Women in Logic Workshop. Cap Hornu, France, Vancouver, Canada, June 23, 2019.

Frank D. Valencia is/has been a member of the program committees of the following conferences and workshops:

CP-DP-19: Doctoral Program of the 25th International Conference on Principles and Practice of Constraint Programming. Stamford, CT, USA, Sep 30 - Oct 4, 2019.

CONCUR 2019: The 30th International Conference on Concurrency Theory. Amsterdam, Netherlands, August 26-31, 2019.

AAMAS 2019: International Conference on Autonomous Agents and Multiagent Systems. Montreal, Canada, 13th-17th of May 2019.

### 9.1.3. Journals

*9.1.3.1. Member of the editorial board*

Catuscia Palamidessi is:

(2019-) Member of the Editorial Board of the Journal of Computer Security IOS Press. Since 2019.

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.

*9.1.3.2. Reviewing*

The members of the team regularly review papers for international journals, conferences and workshops.

### 9.1.4. 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.

### 9.1.5. Participation in other committees

Catuscia Palamidessi has been serving in the following committees:

External Member of the committee for the promotion to full professor of Prof. Kévin Huguenin. HEC Lausanne, Switzerland.

Member of the committee for associate professor positions in the Datalogi Dept., Aalborg Univ., Denmark. 2019.

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 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.

Member of the EAPLS PhD Award Committee. From 2010.

### 9.1.6. Invited talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

Journées Nationales du GDR Sécurité Informatique. Paris, France, June 2019.

MFPS XXXV, special session on Probabilistic Programming. London, UK, June 2019.

AI & Society: From principles to practice. CIFAR-UKRI-CNRS workshop. London, UK, June 2019.

5th France-Japan Cybersecurity workshop}. Kyoto, Japan, April 2019.

Frank Valencia has given the following invited talk:

- EXPRESS/SOS 2019. Combined 26th International Workshop on Expressiveness in Concurrency and 16th Workshop on Structural Operational Semantics. Amsterdam, Netherlands, August 26, 2019.

### 9.1.7. Service

Catuscia Palamidessi has served as:

Member of the committee for the assignment of the Inria International Chairs. From 2017.

Member of the Commission Scientifique du Centre de Recherche Inria Saclay. From 2018.

Member of the hiring committee for Maitre de Conference, Ecole Polytechnique, 2019.

Frank Valencia has served as:

Directeur adjoint de l'UMR 7161, le Laboratoire d'Informatique de l'Ecole Polytechnique (LIX). May 2016 - Nov 2019.

## 9.2. Teaching - Supervision - Juries

### 9.2.1. 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, 2019.

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, 2019

Master : Catuscia Palamidessi has been teaching the masters course on "Foundations of Privacy", 24 hours, at the MPRI, Sept-Nov 2019.

### 9.2.2. Supervision

PhD in progress (2019-) Federica Granese. Co-supervised Catuscia Palamidessi and Daniele Gorla. Thesis subject: Security in Machine Learning.

PhD in progress (2019-) Ganesh Del Grosso. Co-supervised by Catuscia Palamidessi and Pablo Piantanida. Thesis Subject: Privacy in Machine Learning.

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 in progress (2017-) Sergio Ramirez. Co-supervised by Frank Valencia and Camilo Rueda, Universidad Javeriana Cali. Thesis subject: Quantitive Spatial Constraint Systems.

### 9.2.3. Juries

Catuscia Palamidessi has been reviewer and member of the board at the PhD defense for the thesis of the following PhD student:

Mohamed Maouche (INSA, Lyon). PhD thesis reviewer and member of the committee board at the PhD defense. Title of the thesis: *Protection against Re-identification Attacks in Location Privacy*. Defended in November 2019.

Raphaëlle Crubrillé (IRIF, Université Paris Diderot). Member of the committee board at the PhD defense. Title of the thesis: *Distances comportementales pour les programmes probabilistes d'ordre supérieur*. Defended in June 2019.

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.

### 9.2.4. Other didactical duties

Catuscia Palamidessi has been:

External member of the scientific council for the PhD in Computer Science at the University of Pisa, Italy. Since 2012.

## 9.3. Popularization

### 9.3.1. 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 on fairness, Interpretability, and Privacy in AI at the CIFAR-UKRI-CNRS workshop. London, June 2019.

Frank Valencia has:

- Welcomed the students of bachelor program of École Polytechnique to Inria center. Sept 12, 2019.

- Welcomed visitors from ACOFI, the Colombian Association of Faculties of Engineering to Inria center. April 8, 2019.

### 9.3.2. Interventions

Catuscia Palamidessi has given an invited talk at:

- Safety and AI. DATAIA Workshop. Palaiseau, France, September 2019.

## DATASPHERE Team

# 9. Dissemination

## 9.1. Promoting Scientific Activities

Stéphane Grumbach has been co-director of IXXI since 2014. He is also involved in the Anthropocene Group at ENS Lyon, which 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.

### 9.1.1. Scientific Events: Selection

*9.1.1.1. Member of the Conference Program Committees*

Kavé Salamatian has been TPC member for the below conferences:
- Infocom 2020
- Infocom 2019
- Aintec 2019

### 9.1.2. Journal

*9.1.2.1. Reviewer - Reviewing Activities*

Kavé Salamatian has been reviewer for the below journals:
- IEEE/ACM Transactions on Networking
- IEEE Transactions on Communication
- IEEE Transactions on Networked Systems Management
- Computer Communications
- IEEE transactions on Information Theory

## 9.2. Teaching - Supervision - Juries

### 9.2.1. 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.

### 9.2.2. Supervision

PhD: Jingxiu Su, DNS data analysis, 2016-2019, directeur de thèse Kave Salamatian. Defense 30/12/2019

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, co-Directors: Frederick Douzet, Kavé Salamatian

Phd in progress: Xinyi Zhang, IA and cybersecurity, 2019-, Advisor: Kavé Salamatian

Phd in progress: Ali Marandi, Efficient diffusion in NDN, 2016-2020, Advisor: Kavé Salamatian

## 9.3. Popularization

Various publications have appeared in journals accessible to a larger audience. In particular, our research work has been featured in a full page of Le Monde newspaper in July 2019 (https://www.lemonde.fr/international/visuel/2018/07/23/cyberespace-la-guerre-mondiale-des-donnees_5334901_3210.html).

Kavé Salamatian did several radio intervention, in particular, he was invited in the "Methode Scientifique" broadcasting program in November 2019.

<h1 style="text-align:center;color:red">PESTO Project-Team</h1>

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events Organisation

*10.1.1.1. General Chair, Scientific Chair*

- V. Cortier: vice-chair of the ACM Special Interest Group on Logic and Computation (SigLog); vice-chair of the IFIP Wg-1.7 Foundations of Security Analysis.
- J. Dreier: GRSRD 2019, Grande Region Security and Reliability Day 2019, Nancy, March 2019 (chair)

### 10.1.2. Scientific Events Selection

*10.1.2.1. Member of the Conference Program Committees*

- V. Cortier: POST 2019, E-VoteID 2019 (Track chair), S&P 2019, CSF 2019, Voting 2020, Concur 2020, S&P 2020
- V. Cheval: CSF 2020
- J. Dreier: SEC@SAC 2020, 5G-NS 2019, SP5G@ICISSP 2020
- L. Hirschi: SEC@SAC 2020
- A. Imine : ICEIS 2019, DEXA 2019, VLIoT@VLDB 2019, C2SI 2019
- S. Kremer: Euro S&P 2019, Voting 2019, PERR 2019, ESORICS 2019, FSTTCS 2019, CSF 2020, Euro S&P 2020, Voting 2020
- C. Ringeissen: UNIF 2019, FroCoS 2019, WRLA 2020, IJCAR 2020, UNIF 2020
- M. Rusinowitch: IWSPA 2019, STM 2019, CRISIS 2019, IWSPA 2020

### 10.1.3. Journal

*10.1.3.1. Editor in Chief*

- V. Cortier: Journal of Computer Security (EiC since November 2019)

*10.1.3.2. 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

### 10.1.4. Invited Talks

- V. Cortier. Keynote speaker at the ACM SIGSAC 14th Workshop on Programming Languages and Analysis for Security (PLAS 2019), London, UK, November 2019.
- V. Cortier. Keynote speaker at the 24th European Symposium on Research in Computer Security (Esorics 2019), Luxembourg, September 2019.
- V. Cortier. Plenary talk at the 28th edition of Computer Science Logic (CSL 2020), Barcelona, Spain, January 2020.
- S. Kremer. Keynote speaker at the ACM SIGSAC 14th Workshop on Programming Languages and Analysis for Security (PLAS 2019), London, UK, November 2019.
- V. Cheval. Invited talk at the Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, RESSI 2019, Erquy, France, May 2019.

### 10.1.5. Scientific Expertise

- V. Cortier: Member of the W&T5ASP panel of the Research Foundation - Flanders (FWO), Belgium
- A. Imine: ANR project expertise
- L. Hirschi: ANR project expertise
- M. Rusinowitch: FNRS project expertises, Belgium

### 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 Paris (S. Kremer)
Computer science commission of the Doctoral School, Univ Lorraine (L. Vigneron, chair)
Jury Associate Professor at IT University Copenhagen (J. Dreier)
Jury Assistant Professor at EISTI school/ETIS laboratory, Cergy (J. Dreier)
Scientific Council of the Computer Science CNRS Institute INS2I (V. Cortier)

## 10.2. Teaching - Supervision - Juries

### 10.2.1. Teaching

- Licence:

  V. Cheval, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 38 hours (ETD), TELECOM Nancy

  J. Dreier, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 38 hours (ETD), TELECOM Nancy

  J. Dreier, Awareness for Cybersecurity, 7.5 hours (ETD), TELECOM Nancy

  L. Hirschi, Introduction to Theoretical Computer Science (Logic, Languages, Automata), 38 hours (ETD), TELECOM Nancy

- Master:

  V. Cortier, Security of flows, 16 hours, M2 Computer Science, TELECOM Nancy and Mines Nancy

  V. Cortier, Security of flows, 8 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, 24 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Security of information systems, 32 hours (ETD), M2 Computer science, Univ Lorraine

  L. Vigneron, Advanced Security, 28 hours (ETD), Polytech Nancy – Information Systems and Networks, Univ Lorraine

  L. Vigneron, Security of information systems, 16 hours (ETD), M2 MIAGE – Audit and Design of Information Systems, Univ Lorraine

- Summer School:

  V. Cortier. Models and Techniques for Analysing Security Protocols, Winter School of the VMCAI 2019 conference, Cascais/Lisbon, Portugal, January 2019.

### 10.2.2. Supervision

- PhD defended in 2019:

  Joseph Lallemand, Electronic Voting: Definitions and Analysis Techniques [8], November 2019 (V. Cortier)

- 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)

  Itsaka Rakotonirina, Efficient verification of equivalence properties in cryptographic protocols, started in October 2017 (V. Cheval and S. Kremer)

### 10.2.3. Juries

Jury member for J. M. López Becerra, University of Luxembourg (S. Kremer).

Jury president for Hoang-Long Nguyen, University of Lorraine (M. Rusinowitch)

## 10.3. Popularization

### 10.3.1. Articles and contents

Véronique Cortier. Some interactions (in collaboration with P. Gaudry and S. Glondu) with France Culture to improve an online article on e-voting.

Steve Kremer co-authored (with L. Mé, D. Rémy and V. Roca) Inria's White Book on Cybersecurity [27].

Steve Kremer In Horizon - The EU Research and Innovation Magazine: Online voting isn't ready for high-stakes elections, Avril 2019.

Steve Kremer, Ludovic Mé, Didier Rémy, and Vincent Roca. In Blog Binaire - Le Monde. La cybersécurité aux multiples facettes.

Steve Kremer. Le vote électronique. Chapter of the book "Treize défis pour la Cybersécurité" édited by CNRS. To appear in January 2020.

Interview with Science & Vie Junior about 5G security (J. Dreier, in "Pourquoi la 5G va tout changer", Science & Vie Junior, Juillet 2019)

Lucca Hirschi, Ralf Sasse, Jannik Dreier in ERCIM News 2019. "Security Issues in the 5G Standard and How Formal Methods Come to the Rescue".

### 10.3.2. Interventions

Invited conference at the Espace des sciences, Rennes (audience of about 300 people, 5K+ views on Youtube), October, 22nd, 2019 (V. Cortier)

"breakfast" in the Senat, on Cybersecurity, organized by OPECST / Académie des sciences / Académie de médecine, June 19th, 2019. (V. Cortier)

How to explain security protocols with Playmobil, group of high school students interns for a week, February 3rd, 2019, (V. Cortier)

<span style="color:red">**PRIVATICS Project-Team**</span>

# 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, 10/10/2018, Lyon, France.

Claude Castelluccia: *AI & Information Disorder* as part of the Global Forum on AI for Humanity forum, October 2019, Paris, France.

*8.1.1.2. Member of the Organizing Committees*

Antoine Boutet: Workshop on data transparency, 10/10/2019, Lyon, France.

Antoine Boutet: Winter School on Distributed Systems and Networks 2019, 4-8/02/2019, Sept Laux, France.

Antoine Boutet: SRDS 2019, 01-04/10/19 Lyon, France.

Daniel Le Métayer: Panel *Influence or manipulation? What protections in the digital world?*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Claude Castelluccia, *Building trust in AI, building trust with AI*, Global Science Week, 01/06/2019, Grenoble, France.

### 8.1.2. Scientific Events Selection

*8.1.2.1. Member of the Conference Program Committees*

Antoine Boutet: Social Network Analysis and Mining 2019, Nature 2019, MDPI 2019, IEEE Transactions on Services Computing 2019, APVP 2019, Compas 2019, Location Privacy Workshop 2019.

Mathieu Cunche: ACM WiSec 2019, APVP 2019, AlgoTel 2019, IEEE WCNC 2019.

Claude Castelluccia: APF 2019.

Cédric Lauradoux: ACM CCSW 2019, Prix Gilles Kahn.

Daniel Le Métayer: XAI 2019, IWPE 2019, CPDP 2019, APF 2019.

Vincent Roca: SPACOMM 2019.

### 8.1.3. Invited Talks

Claude Castelluccia, *A Risk Analysis Framework for Facial Recognition Applications*, MIAI chair on AI&Ethics (T. Menissier), 04/12/2019, Grenoble, France.

Claude Castelluccia, *Cognitive security*, closing the regulatory gap for consumer neurotechnology" workshop, Brocher Fondation, 25-27/11/2019, Geneva, Switzerland.

Claude Castelluccia, *Influence or manipulation ? What protections in the digital world? (panel)*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Cédric Lauradoux, *Subject Access Request and Proof of Ownership*, SoSySec Seminar, 25/10/2019, Rennes, France.

Cédric Lauradoux, *Influence or manipulation ? What protections in the digital world? (panel)*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Cédric Lauradoux, *Y-aura-t-il un Cambridge Analytica de nos data santé ? (panel)*, FUTUR.E.S, 13/06/2019, Paris, France.

Cédric Lauradoux, *Pseudonymisation*, École de Cybersécurité de l'Université de Nice, 09/07/2019, Nice, France.

Cédric Lauradoux, *Subject Access Right*, Laboratoire d'Innovation Numérique de la CNIL, 12/07/2019, Paris, France.

Cédric Lauradoux, *Subject Access Request and Proof of Ownership*, CyberAlps Workshop on GDPR, 09/10/2019, Grenoble, France.

Daniel Le Métayer, *Inaugural session: How to promote a responsable design and usage of decision making systems ?* , Center for Internet and Society, 27/09/2019, Paris, France.

Daniel Le Métayer and Clément Hénin *Social Responsability of Algorithms*, SRA 2019, 12/12/2019, Paris, France.

Daniel Le Métayer, *HumanAI*, workshop on transparency and accountability for algorithmic decision systems, 11/09/2019, Montreal, Canada.

Mathieu Cunche, *Mécanismes anti-traçage dans les réseaux sans-fil*, journées nationales du GDR sécurité 2019, 12/06/19, Paris, France.

Vincent Roca, *Vers un habitat intelligent... mais fortement indiscret : la maison connectée sous l'angle de la vie privée*, Séminaire "Vie privée, mobile et sécurité", Festival des Libertés Numériques, 06/02/2019, Rennes, France.

## 8.2. Teaching - Supervision - Juries

### 8.2.1. Teaching

Master : Antoine Boutet, *Security and Privacy*, 14h, INSA-Lyon, France.

Master : Antoine Boutet, *Security and Privacy 16h*, Polytech Annecy, France.

Undergraduate course: Antoine Boutet, *System and Network*, 160h, L3, INSA-Lyon, France.

Master: Antoine Boutet, *Network, 24h*, Polytech Annecy, 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 Métayer, *Privacy*, 12h, M2 MASH, Université Paris Dauphine, France.

Master : Daniel Le Métayer, *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*, 3h, L-Pro, University of Grenoble Alpes, France.

Undergraduate course : Vincent Roca, *C-Language Programming*, 24h, L-Pro, University of Grenoble Alpes, France.

Master : Vincent Roca, *On Security and Privacy in smartphones*, 3h, M2, France.

## 8.2.2. E-learning

### MOOC "Protection de la vie privée dans le monde numérique:"

Nataliia Bielova, Cédric Lauradoux, Vincent Roca, Session 3, (open during 2 months), FUN-MOOC, Inria, public targeted: around 30000 for the three sessions since 2018, https://www.fun-mooc.fr/courses/course-v1:inria+41015+session03/about.

## 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* , April 2017, Vincent Roca with Arnaud Legout (DIANA Inria team).
- 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 Métayer.
- PhD in progress: Théo Jourdan, *Privacy-preserving machine learning in medical domain, October 2018, Antoine Boutet.*
- *PhD in progress : Michale Toth,* Privacy protection of Web users and compliance with GDPR and ePrivacy Regulations *, December 2019, Natallia Bielova and Vincent Roca.*
- *Intern (M2): Michael Toth ,* Analyse et présentation accessible aux utilisateurs de Chartes de Vie Privée dans le contexte du RGPD, Vincent Roca.
- Intern (M2): Piyush Patil, *Privacy Leak Analysis in the Context of Smart Homes, Vincent Roca.*
- *Intern (M1): Jan Aalmoes - Understanding how location data influences personalized content in the mobile context, Antoine Boutet.*
- *Intern (M1): Vincent Prax - Privacy Analysis of Email Providers, Cédric Lauradoux.*
- *Intern (L3): Félix Fonteneau - Activity recognition using federated learning, Antoine Boutet.*
- *Intern (L3): Hilaire Bouaddi - Analysis of mobility traces, Antoine Boutet.*
- *Intern (L3): Amine Bahi - Privacy-preserving and scalable machine learning using homomorphic encryption, Antoine Boutet.*

## 8.2.4. Juries

HDR: Carole Frindel, *Approche computationnelle de l'imagerie médicale : application en neurosciences*, INSA Lyon, France, 13/12/2019, Claude Castelluccia.

PhD: Pieter Robyns, *Explicit and Implicit Information Leakage in Wireless Communication*, 11/12/19, Hasselt University, Belgium, Mathieu Cunche (reviewer).

PhD: Timothy CLAEYS, *Security for the Internet of Things: A bottom-up approach to the secure and standardized Internet of Things*, 19/12/19, Université de Grenoble Alpes, France, Mathieu Cunche (examiner).

PhD: Antoine Vastel, *Tracking versus security: investigating the two facets of browser fingerprinting*, Université de Lille, France, 23/10/2019, Daniel Le Métayer.

PhD: Julien Loudet, *Distributed and privacy-preserving personal queries on personal clouds*, Universitée Paris-Saclay, thèse préparée à Université de Versailles Saint-Quentin-en-Yvelines, 24/10/2019, France, Vincent Roca (reviewer).

## 8.3. Popularization

### 8.3.1. Hearings

- Claude Castelluccia: *audition at the Council of Europe on AI & Human Rights*, European Parliament, 05/2019, 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).
- Claude Castelluccia is a member of the Grenoble AI institute (MIAI)
- Daniel Le Métayer is a member of the European Commission Multistakeholder expert group to support the application of General Data Protection Regulation (GDPR).
- Daniel Le Métayer is Chair of the CNIL-Inria privacy award.
- Daniel Le Métayer is a member of the steering committee of APVP (Atelier Protection de la Vie Privée).
- Daniel Le Métayer is a member of the steering committee of the chair « Transformation de l'action publique » of Sciences Po Lyon.
- Antoine Boutet is the communication manager of CITI laboratory.
- Antoine Boutet is the manager the Cybersecurity and privacy option of the 5th year of computer science at INSA-Lyon.
- Cédric Lauradoux is a representative of Inria ethical committee COERLE at Inria Grenoble Rhone-Alpes.
- Cédric Lauradoux is a member of the scientific committee of the research action "Cyber-Physical System" of Labex Persyval (Grenoble).
- Cédric Lauradoux is a member of the ethics committee of ComUE Université Grenoble Alpes.
- Cédric Lauradoux is a member of Inria Grenoble Rhône-Alpes committee for technological development.
- Vincent Roca is the PRIVATICS Team Leader (since Nov. 2020).
- Vincent Roca is the co-chair of the NWCRG ("Coding for Efficient Network Communications" Research Group), Internet Research Task Force (IRTF) / IETF.
- Vincent Roca is the ANR 2017 DAPCODS/IOTics project leader.
- Vincent Roca is the chair of the CUMI ("Commision des Utilisateurs des Moyens Informatiques") of Inria Grenoble Rhone-Alpes.

- Vincent Roca is a member of Inria ethical committee COERLE.
- Vincent Roca is co-editor (with Ludovic Mé and Steve Kremer) of a series of articles dedicated to cybersecurity on the Blog Binaire, Le Monde.

### 8.3.3. Articles and contents

- Antoine Boutet et Mathieu Cunche: *Souriez, vous êtes géolocalisés !*, "Tout compte fait", 06/05/2019
- Antoine Boutet: *L'algorithme : cette formule arbitraire, miroir de l'intention humaine*, En Vue (INSA Lyon newsletter), 18/12/2019 .
- Claude Castelluccia: *Manipulation informationnelle et psychologique*, Le blog binaire du Monde, 05/2018.
- Mathieu Cunche: *Des chercheurs français découvrent des fuites d'informations sensibles sur les appareils Apple*, Science et Avenir.fr, 16/12/2019.
- Mathieu Cunche, *Vers une reconnaissance faciale généralisée*, Techniques de l'ingénieur, 05/12/2019.
- Cédric Lauradoux, *Bientot un identifiant numérique pour tous*, Les Echos, 07/05/2019.
- Cédric Lauradoux, *Facebook, mon fil d'actu, ma bataille*, Mediapart, 05/12/2019.
- Daniel Le Métayer and Claude Castelluccia: *Algorithmic decision making : risks and opportunities for society*, Inria Interview, 25/06/2019.
- Daniel Le Métayer: *Interview about algorithmic decision systems.*, Atlantico, 21/09/2019.
- Vincent Roca and Cédric Lauradoux: *Prêts à tout pour protéger leurs données*, 01NET, 02/10/2019.
- Vincent Roca: *Suite au Livre Blanc Inria sur la cybersécurité : L'ordinateur quantique est une menace pour une partie des techniques de chiffrement actuellement utilisée*, L'Hebdo, BFM Business, 09/02/2019.
- Vincent Roca: *Les objets connecte´s nous espionnent-ils ?*, "Les Idées Claires", France Culture, 12/03/2019.
- Vincent Roca: *Rencontre Sciences et Politique : Cybersécurité*, Acade´mie des sciences - Acade´mie nationale de me´decine - Office parlementaire d'e´valuation des choix scientifiques et technologiques (OPECST), Sénat, 19/06/2019.
- Vincent Roca: *Objets connectés et vie privée*, Les Echos, 20/03/2019.
- Vincent Roca: *Nouvelles technologies : tous espionnés*, Journal de 20 Heures, France 2, 12/04/2019.
- Vincent Roca: *Vie privée et maison intelligente*, Café des Sciences, 14/05/2019, Grenoble, France.

### 8.3.4. Education

- Nataliia Bielova: *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.
- Antoine Boutet: Contest of data anonymization between three different groups of INSA students (from Lyon and Bourges), 25-26/11/19.
- Cédric Lauradoux: *Action vie privée*, Maison pour la science, 14/02/2019, Grenoble, France.
- Cédric Lauradoux: *Protéger sa vie privée*, DIU EIL (enseignant d'informatique au lycée), 12/04/2019, Grenoble, France.
- Cédric Lauradoux: *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.
- Vincent Roca: : *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.

### 8.3.5. Interventions

- Mathieu Cunche: *Cybersécurité: Protéger ses objets physiques*, Pint of science, 22/05/2019, Lyon, France.
- Cédric Lauradoux: *Procès du robot 42*, Festival TRANSFO, 24/01/2019, Grenoble, France.
- Cédric Lauradoux: *Challenges de cryptologie*, Printemps du numérique, 08/04/19, Die, France.
- Cédric Lauradoux: *Challenges de cryptologie*, MathC2+ internship, 25/06/19, Grenoble, France.
- Cédric Lauradoux: *Atelier cryptographie*, Fête de la Science, 10/10/2019, Grenoble, France.
- Cédric Lauradoux: *Procès du robot 42*, Fête de la Science, 12/10/2019, Grenoble, France.
- Cédric Lauradoux: *Les données en question*, Festival Imaginascience, 16/10/2019, Annecy, France.
- Cédric Lauradoux: *Le Numérique nous menace-t-il ?*, Telecom Saint Etienne, 03/12/2019, Saint Etienne, France.
- Cédric Lauradoux: *Vie privée et Liberté dans le monde numérique*, Collège Les Dauphins, 03/12/2019, Saint Jean de Soudain, France.
- Cédric Lauradoux: *Challenges de cryptologie*, Cité scolaire Jean PREVOST, 12/12/2019, Villard de Lans, France.
- Cédric Lauradoux: *Avoir un usage Internet éclairé*, UIAD, 18/12/2019, Grenoble, France.
- Vincent Roca: *Maison intelligente : le point de vue du respect de la vie privée*, Café des Sciences, 14/05/2019, Grenoble, France.
- Vincent Roca: *Habitat intelligent, service de vélo partagé et vie privée*, Fête de la Science, 12/10/2019, Grenoble, France.

## 8.3.6. Internal action

- Cédric Lauradoux: *Formation Éthique*, Inria Paris, 26/01/2019, Paris, France.
- Cédric Lauradoux: *Formation Éthique*, Inria Saclay, 25/04/2019, Saclay, France.
- Cédric Lauradoux: *Formation Éthique*, Inria Grenoble - Rhône-Alpes, 13/05/2019, Lyon, France.
- Cédric Lauradoux: *Rules of Cyber Engagement*, Inria JSI, 07/06/2019, Lyon, France.
- Cédric Lauradoux: *Privacy: Understanding the GDPR*, Inria Grenoble - Rhône-Alpes, 15/10/2019, Grenoble, France.
- Vincent Roca: *Sécurité numérique : technique, éthique, juridique : qui s'y frotte s'y pique (moderator)*, Inria JSI, 07/06/2019, Lyon, France.

## PROSECCO Project-Team

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### 10.1.1. Scientific Events: Organisation

*10.1.1.1. General Chair, Scientific Chair*

- Catalin Hritcu is the Steering Committee Chair of the Workshop on Principles of Secure Compilation (PriSC)
- Catalin Hritcu is the main organizer a Dagstuhl Seminar on Secure Compilation (20201)
- Karthikeyan Bhargavan co-chaired the Workshop on Secure Messaging at EUROCRYPT 2019

*10.1.1.2. Member of the Organizing Committees*

- Catalin Hritcu is a Steering Committee Member of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP)

### 10.1.2. Scientific Events: Selection

*10.1.2.1. Chair of Conference Program Committees*

- Catalin Hritcu served as Program Chair of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP)

*10.1.2.2. Member of the Conference Program Committees*

- Karthikeyan Bhargavan was PC member of CCS 2019
- Bruno Blanchet was PC member of CSF 2019
- Catalin Hritcu was PC member of RV 2019, SecDev 2019, CSF 2020

### 10.1.3. Journal

*10.1.3.1. Member of the Editorial Boards*

Associate Editor

– of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers: Bruno Blanchet

### 10.1.4. Invited Talks

- Karthikeyan Bhargavan gave invited talks at ERCIM Rome, FSTTCS Mumbai, ICISS Hyderabad,
- Catalin Hritcu gave invited talks at EPFL Lausanne, Ruhr University Bochum, MPI-SWS, and Chalmers University;

### 10.1.5. Leadership within the Scientific Community

- Catalin Hritcu served as the Artifact Evaluation Co-Chair for POPL 2018 and POPL 2019

### 10.1.6. 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 was a scientific consultant for Nomadic Labs, regarding the development of the blockchain Tezos.
- Karthikeyan Bhargavan was scientific consultant for Nomadic Labs, regarding verified cryptographic software.

### *10.1.7. Research Administration*

- Bruno Blanchet was a member of the hiring scientific jury for Inria researchers (*chargé de recherche*) of the Inria Paris center.
- Bruno Blanchet was a representative of Inria Paris at the DIM RFSI (*Domaine d'Intérêt Majeur, Réseau Francilien en Sciences Informatiques*).

## 10.2. Teaching - Supervision - Juries

### *10.2.1. Teaching*

- Master: Bruno Blanchet, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII
- Master: Karthikeyan Bhargavan, Cryptographic protocols: formal and computational proofs, 18h equivalent TD, master M2 MPRI, université Paris VII
- PhD: Karthikeyan Bhargavan, Verified Crypto for Verified Protocols, Sibenik Summer School on real-world crypto and privacy, 17-21 June, 2019
- PhD: Catalin Hritcu, Program Verification with F* course at Summer School on Verification Technology, Systems, and Applications, VSTA 2019, 1-5 July 2019 at University of Luxembourg
- PhD: Catalin Hritcu, Writing and Verifying Functional Programs in Coq course at Summer School on Cryptography, Blockchain, and Program Verification, Mathinfoly 2019, 24-31 August 2019 at INSA, Lyon

### *10.2.2. Supervision*

- 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: Benjamin Beurdouche, Formal Verification for Real-World Cryptographic Protocols, PSL, since September 2016, supervised by Karthikeyan Bhargavan.
- PhD in progress: Natalia Kulatova, Formal Analysis of Security Devices, PSL, since September 2017, supervised by Karthikeyan Bhargavan and Graham Steel.
- PhD in progress: Marina Polubelova, Formal Verification of a Cryptographic Library, PSL, since September 2017, supervised by Karthikeyan Bhargavan.
- PhD in progress: Denis Merigoux, Verification framework for performance-oriented memory-safe programming languages, since September 2018, supervised by Karthikeyan Bhargavan and Jonathan Protzenko.
- PhD: Kenji Maillard, on Principles of Program Verification for Arbitrary Monadic Effects, started January 2017, supervised by Catalin Hritcu
- PhD in progress: Carmine Abate, The Formal Foundations of Secure Compilation, since June 2018, advised by Catalin Hritcu
- PhD in progress: Jérémy Thibault, Secure Compartmentalizing Compilation to a Tagged Architecture, from August 2018, advised by Catalin Hritcu
- 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

### *10.2.3. Juries*

- Bruno Blanchet was member of the PhD jury of Adrien Koutsos (ENS Paris-Saclay).
- Karthikeyan Bhargavan was member of the PhD jury of Joseph Lallemand (Univ. Lorraine) and Guido Martinez (Univ Stuttgart).

- Catalin Hritcu was a discussion leader for the Licentiate defense of Maximilian Algehed (Chalmers University);

## 10.3. Popularization

### 10.3.1. Articles and contents

- Catalin Hritcu contributed an article on Secure Compilation to the SIGPLAN PL Perspectives blog
- Karthikeyan Bhargavan published a paper in Communications of the ACM

<p align="center" style="color:red"><b>TAMIS Project-Team</b></p>

# 9. Dissemination

## 9.1. Promoting Scientific Activities

### 9.1.1. Scientific Events: Selection

*9.1.1.1. 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)

*9.1.1.2. Member of the Conference Program Committees*

Annelie Heuser was a member of the following conference program committees: CARDIS 2019, COSADE 2019, PROOFS 2019.
Olivier Zendra was a member of the program committee of ICOOOLPS 2019.

*9.1.1.3. Reviewer*

Tania Richmond was a reviewer for TCHES 2019 and TCHES 2020.
Alexandre Gonzalvez was a reviewer for TCHES 2019.
Matthieu Mastio was a reviewer for DATE2020.

### 9.1.2. Journal

*9.1.2.1. Member of the Editorial Boards*

Annelie Heuser was a member of TCHES 2019.

*9.1.2.2. Reviewer - Reviewing Activities*

Annelie Heuser was a reviewer of several papers in Journal of Cryptographic Engineering, Transactions on Information Forensics & Security, IEEE Transactions on Circuits and Systems, Transactions on Information Forensics & Security.
Tania Richmond was a reviewer for Transactions on Information Forensics and Security (TIFS)

### 9.1.3. Invited Talks

Annelie Heuser was invited to present at the seminar of Paris 8 on "Mathématiques Discrètes, Workshop Workshop on Randomness and Arithmetics for Cryptography on Hardware, Codes et Cryptographie", GDR Sécurité - Sécurité, fiabilité et test des SoC2, the Summer School on real-world crypto and privacy.
Annelie Heuser was invited to the Dagstuhl seminar on Secure Composition for Hardware Systems.
Annelie Heuser was invited to the Lorentzcenter on AI+Sec: Artificial Intelligence and Security, and SHARD: Bridging the Gap Between Software and Hardware Security.

### 9.1.4. Expertise

Tania Richmond reviewed for the HiPEAC Collaboration Grants 2019.
Annelie Heuser reviewed an application to receive a national application grant (inside Europe).
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 is a member of the editorial board and co-author of the "HiPEAC Vision 2021"

### 9.1.5. Research Administration

Olivier Zendra is a member of Inria's evaluation committee.

## 9.2. Teaching - Supervision - Juries

### *9.2.1. Teaching*

Christophe Genevey-Metat taught:

- Programming in Java to Licence 1, University Rennes 1,
- Introduction at Security to Master 1, University Rennes 1.

Cassius de Oliveira Puodzius taught:

- 24h of Reverse Engineering + Malware analysis for the Introduction at Security to Master1 at Rennes 1,
- 6h of Java Programming to Licence1 at ECAM Rennes.

Tania Richmond taught Physical Attacks in "Préparation à l'Agrégation" en Sciences de l'Ingénieur, ENS Rennes.

### *9.2.2. Supervision*

- PhD in progress: Christophe Genevey Metat (Rennes 1): , October 2018, Jean-Marc Jezequel, Benoit Gerard, Annelie Heuser and Clementine Maurice
- PhD in progress : Alexandre Gonzalvez, On Obfuscation via crypto primitives, April 2016, Caroline Fontaine.
- PhD defended in 2019 : Nisrine Jafri (Rennes1), On fault Injection detection with MC of Binary code, Axel Legay and Jean-Louis Lanet.
- PhD in progress : Tristan Ninet (Rennes 1), Vérification formelle d'une implémentation de la pile protocolaire IKEv2, December 2016, Stéphanie Delaune, Romaric Maillard and Olivier Zendra
- PhD in progress: Lamine Nouredine (Rennes1); Automatic techniques for packing detection, classification and unpacking to stop malware propagation, November 2017, Stephane Ubeda, Olivier Zendra, Annelie Heuser.
- PhD in progress: Cassius de Oliveira Puodzius (Rennes1); Threat malware analysis, February 2019, Ludovic Me, Olivier Zendra, Annelie Heuser.
- PhD in progress: Duc Phuc Pham (Rennes1); Malware analysis through side-channel information, May 2019, Jean-Louis Lanet, Annelie Heuser, Olivier Zendra.

### *9.2.3. Juries*

- Annelie Heuser was a referee for the PhD defense of Nisrine Jafri (University Rennes).
- Olivier Zendra was a member of the jury for the PhD defense of Delphine Beaulaton at University of Southern Brittany in Vannes.