informatics *mathematics*

Inria

RESEARCH CENTER

FIELD
Algorithmics, Programming, Software and Architecture

Activity Report 2012

Section Dissemination

ARIC Team

9. Dissemination

9.1. Scientific Animation

- Florent de Dinechin was in the program committee of HEART 2012 (Highly Efficient Accelerators for Reconfigurable Computing), FPL 2012 (Field-Programmable Logic), FPT 2012 (Field-Programmable Technologies) and ARC 2012 (Applied Reconfigurable Computing), and on the steering committee of the french Symposium on Architectures.

- Guillaume Hanrot was in the hiring committees for professors at the universities of Caen, Toulon, and UCB Lyon 1. He is a member of the scientific council of ENSIIE (Évry).

- Claude-Pierre Jeannerod, Nicolas Louvet, Nathalie Revol, Dave Saunders (University of Delaware, U.S.A.), Philippe Théveny and Gilles Villard organized the LyonBox meeting that gathered members of the LinBox project (ENS de Lyon, July 19-21).

- Claude-Pierre Jeannerod was in the software exhibits committee of ISSAC 2012. He is also a member of the scientific committee of "Journées Nationales de Calcul Formel".

- Fabien Laguillaumie was in the program committee of ACISP 2012 (17th Australasian Conference on Information Security and Privacy).

- Jean-Michel Muller chaired the Aeres visiting committees of laboratories LIAFA and PPS. He was in the program committee of ARITH'21 (21st IEEE Symposium on Computer Arithmetic) and ASAP'2012 (Application-Specific Systems, Architectures and Processors). He is a member of the scientific councils of École Normale Supérieure de Lyon and Cerfacs.

- Nathalie Revol is a member of the steering and scientific committees of SCAN 2012, Novosibirsk. She organized a session on interval arithmetic at RAIM 2012, Dijon. She is a member of the "comité de diffusion" of the MILyon labex, one of her tasks was the selection of participants to ISSMYS 2012, Lyon. She is a member of the selecting committee of CapMaths. She is a member of the CES (Commission des Emplois Scientifiques), the hiring committee for postdocs at Inria Grenoble - Rhône-Alpes.

- Bruno Salvy is a member of the editorial boards of the Journal of Symbolic Computation and of the Journal of Algebra (section Computational Algebra), as well as the Springer series "Texts and Monographs in Symbolic Computation" and the series "Mathématiques & Applications" of the French SMAI. He is organizing the working group Computer Algebra of the CNRS GDR IM (Mathematical Computer Science). This year, he is a member of the program committee of AofA 2012 (Analysis of Algorithms), Montreal, Analco13 (Analytic Algorithmics and Combinatorics), New Orleans and ISSAC 2013 (Symbolic and Algebraic Computation), Boston. He has also been a member of several committees: PES at Inria; hiring junior researchers (CR) at Inria; hiring professors in Caen and Grenoble; visiting committee of the laboratory Liafa (Paris 7) for the Aeres.

- Damien Stehlé was in the program committees of INDOCRYPT'12, CRYPTO'12 and ISSAC'12. He was in the hiring committees for lecturers at the universities of Grenoble and Montpellier. He is a member of the steering committee of the Cryptography and Coding working group of GDR IM.

- Gilles Villard is chair of LIP laboratory.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Introduction to computer science, 24h, L1, ENS Lyon / classe passerelle pour l'enseignement supérieur, taught by Guillaume Hanrot (autumn 2012)

Licence : Introduction to Functional Programming, 30h, L1, UCB Lyon 1, taught by Nicolas Louvet (autumn 2012);

Licence : Computer Architecture, 74h, L2, UCB Lyon 1, taught by Nicolas Louvet (spring 2012);

Licence : Algorithms and Data Structures, 30h, L3, UCB Lyon 1, taught by Nicolas Louvet (autumn 2012);

Licence : Operating Systems, 60h, L3, UCB Lyon 1, taught by Nicolas Louvet (spring and autumn 2012);

Licence : "Groupe de lecture" Error-Correcting Codes, 24h, L3, ENS Lyon, taught by Nicolas Brisebarre, Eleonora Guerrini, Guillaume Hanrot and Damien Stehlé (spring 2012);

Master: Numerical Algorithms, M2, UCB Lyon 1, 20h taught by Claude-Pierre Jeannerod and 16h taught by Nicolas Louvet in a 36h course (spring 2012);

Master: Formal Proofs of Floating-Point Algorithms, ENS Lyon, 10h taught by Jean-Michel Muller in a 24h course (autumn 2012);

Master: Computer Arithmetic, 30h, M2, UCB Lyon 1, taught by Vincent Lefèvre (autumn 2012);

Master: Approximations: from symbolic to numerical computation, and applications, ENS Lyon, 12h taught by Nicolas Brisebarre and 12h taught by Bruno Salvy in a 24h course (autumn 2012);

Master: Computer Algebra, 24h, M1, ENS Lyon, taught by Guillaume Hanrot and Claude-Pierre Jeannerod (spring 2012);

Introduction to informatics for high school teachers, part of which (16h) was taught by Guillaume Hanrot (spring 2012).

9.2.2. Supervision

PhD & HdR :

PhD: Jingyan Jourdan-Lu, *Custom floating-point arithmetic for integer processors: algorithms, implementation, and selection* [11], ENS de Lyon - Université de Lyon, defended on November 15, 2012. Supervisors: Claude-Pierre Jeannerod, Christophe Monat (STMicroelectronics Compilation Expertise Center, Grenoble), and Jean-Michel Muller.

PhD: Érik Martin-Dorel, *Contributions à la vérification formelle d'algorithmes arithmétiques* [12], ENS de Lyon - Université de Lyon, defended on September 26, 2012. Supervisors: Micaela Mayero and Jean-Michel Muller.

PhD: Adrien Panhaleux, *Contributions à l'arithmétique flottante : codage et arrondi correct de fonctions algébriques* [13], ENS de Lyon - Université de Lyon, defended on June 27, 2012. Supervisors: Nicolas Louvet and Jean-Michel Muller.

PhD in progress : Nicolas Brunie, *Architecture et réalisation d'un accélérateur reconfigurable à couplage fort pour processeurs parallèles*, begun in September 2010 (CIFRE from April 2011), Florent de Dinechin, Renaud Ayrignac (Kalray).

PhD in progress : Julien Devigne, *Chiffrement pour la protection de la vie privée*, begun in September 2011 (Orange Labs - University of Caen), co-supervised by F. Laguillaumie (together with Sébastien Canard and Brigitte Vallée)

PhD in progress: Adeline Langlois, *Foundations of lattice-based cryptography*, begun in September 2010, supervised by D. Stehlé

PhD in progress: Philippe Théveny, *Numerical quality and high performance in scientific computing on emerging architectures*, begun in September 2011, supervised by N. Revol

PhD in progress : Serge Torres, *Some tools for the design of efficient and reliable function evaluation libraries*, started in September 2010, Supervisors: Nicolas Brisebarre and Jean-Michel Muller.

9.2.3. Juries

- Nicolas Brisebarre was a member of the board of examiners for the PhD defense of A. Benoit (École Polytechnique, 2012-07-18).
- Florent de Dinechin was a referee for the PhD of Naeem Abbas (Université Rennes-1, 2012-05-22).
- Guillaume Hanrot chaired the board of examiners for the PhD defense of P. Lezowski (Univ. Bordeaux 1, 2012-12-01).
- Claude-Pierre Jeannerod was in the PhD committee of J. Jourdan-Lu (ENS de Lyon, 2012-11-15).
- Fabien Laguillaumie was in the PhD committees of Kaoutar Elkhiyaoui (EURECOM, 2012-09-12) and Olivier Blazy (ENS de Paris, 2012-09-27) as a referee and of Roch Lescuyer (Orange Labs/ENS de Paris, 2012-11-21).
- Jean-Michel Muller chaired the boards of examiners for the PhD defenses of T.M.T. Nguyen (Univ. Paris Sud, 2012-06-11) and R. Lebreton (École Polytechnique, 2012-12-11), and was a member of the boards of examiners for the PhD defenses of E. Martin-Dorel (ENS Lyon, 2012-09-26), A. Panhaleux (ENS Lyon, 2012-06-27), and J. Jourdan-Lu (ENS Lyon, 2012-11-15), and for the Habilitation defenses of M. Mayero (Univ. Paris Nord, 2012-11-22) and E. Thomé (Univ. Nancy, 2012-12-13).
- Bruno Salvy has been a member of the PhD committees of P.-J. Spaenlauher (Paris 6, 2012-10-09), O. Roussel (Paris 6, 2012-09-25) and of the committee for the habilitation of E. Thomé (Nancy, 2012-12-13), for which he was a referee.
- Damien Stehlé was in the PhD juries of P. Lezowski (Université Bordeaux 1, 2012-12-01) and G. Quintin (Ecole Polytechnique, 2012-11-22), for which he was a referee.

9.3. Invited Conferences

- Florent de Dinechin gave invited lectures at CERFACS (Toulouse), at the CERN/Intel OpenLab workshop at CERN and and at CASPUR (Rome). He gave talks at Altera (High Wycombe, UK) and Maxeler Technologies (London).
- Jean-Michel Muller gave invited talks in satellite workshop of the SIAM'2012 Conference on Applied Linear Algebra (Valencia, Spain, June 2012), in the Workshop on Numerical Software (Santander, Spain, July 2012), and the LMS Colloquium "Verification and Numerical Algorithms" (London, November 2012).
- Nathalie Revol gave invited talks at national meetings: "Précision numérique" at CNES (Toulouse, January 2012), "Précision et incertitudes" organized by the thematic groups GAMNI and MAIRCI of the SMAI (Paris, February 2012), and at international meetings: "IFIP Working Group 2.5 on Numerical Software" and "Numerical software: design, analysis and verification" (both at Santander, Spain, July 2012).
- Damien Stehlé gave an invited talk at the workshop on Mathematical and Statistical Aspects of Cryptography (Kolkata, India, January 2012), lectures at International Workshop on Recent Advances in Lattice Reduction Algorithms and their Applications (Hyderabad, India, April 2012), an invited talk at Journées Charles Hermite (Nancy, France, June 2012), a plenary invited talk at the international conference SCC 2012 (Castro Urdiales, Spain, July 2012), lectures at Ecrypt Summer School on Lattices (Porto, Portugal, October 2012), an invited talk at the workshop on Post-Quantum Cryptography and Quantum Algorithms (Leiden, Netherlands, November 2012) and an invited talk at Colloquium Jacques Morgenstern (Sophia-Antipolis, December 2012).

9.4. Popularization

- Nathalie Revol gives talks for pupils at collèges and lycées, as an incentive to choose scientific careers: lycée Chabrillan (Montélimar, Drôme), collège Jacques Cœur (Lentilly, Rhône). She gave two talks around Women's Day, one at collège Pierre Moreto (Thuir, Pyrénées-Orientales) and one for a general audience, invited by the city of Canohes (Pyrénées-Orientales). The French Ministry of Education launched the first week of mathematics: N. Revol took part in the preparation of a television report for France 2 and whe gave two 2-hours talks at lycées Pierre Brossolette (Villeurbanne) and Juliette Récamier (Lyon). For the Science Fair, she gave two talks at ENS Lyon.

CARAMEL Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. *Caramel seminar*

Twenty speakers were invited to our seminar in 2012: Charles Bouillaguet, Stéphane Glondu, Marion Videau, Jérémie Detrey, Karim Khalfallah, Peter Schwabe, Jean-Charles Faugère, Luc Sanselme, Olivier Levillain, Aurore Guillevic, Cyril Bouvier, Răzvan Bărbulescu, Francisco Rodríguez-Henríquez, Laura Grigori, Hugo Labrande, Christophe Petit, Alexandre Benoit, Paul Zimmermann, Mohab Safey El Din, and Alin Bostan.

9.1.2. *Committees memberships*

- Jérémie Detrey
  - was a member of the program committee of the International Conference on Pairing-Based Cryptography (Pairing 2012),
  - was a member of the program committee of the International Workshop on the Arithmetic of Finite Fields (WAIFI 2012),
  - is a member of the program committee of the *Symposium en Architectures nouvelles de machines* (SympA 2013).
- Pierrick Gaudry
  - is a deputy director of LORIA until the end of 2012,
  - was in the hiring committees (Comités de Sélection) in Paris 6, Montpellier and Nancy,
  - with Cécile Dartyge (IECN), he organized a scientific day "Journée Charles Hermite" on cryptography and number theory,
  - was a member of the program committee of the 13th International Workshop on Information Security Applications (WISA 2012).
- Emmanuel Thomé
  - is an elected member of the Inria Evaluation Committee for the period 2011-2015,
  - was a member of the program committee of the Workshop on Elliptic Curve Cryptography (ECC 2012).
- Marion Videau
  - is a member of the scientific committee of the CCA seminar (*Codage, Cryptologie, Algorithmes*),
  - was a member of the program committee of the International Conference on Information Security and Cryptology (ICISC 2012),
  - is a member of the program committee of the *Symposium sur la sécurité des technologies de l'information et des communications* (SSTIC 2013).
- Paul Zimmermann
  - is an elected member of the Inria Scientific Board,
  - is a member of the program committee of the International Symposium on Symbolic and Algebraic Computation (ISSAC 2013).

9.1.3. *Invited Conferences*

- Jérémie Detrey was invited to give a talk at the Workshop on Elliptic Curve Cryptography (ECC 2012) in Querétaro, México.
- Emmanuel Thomé was invited to give a talk at the International Workshop on the Arithmetic of Finite Fields (WAIFI 2012) in Bochum, Germany.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Jérémie Detrey:

    Security of websites: 2 hours (lecture), L1, IUT Charlemagne, Nancy, France.

- Emmanuel Thomé:

    Cryptology: 20 hours, M1, ESIAL, Nancy, France.

    Algorithmic Number Theory: 9 hours (lectures), M2, University Paris 7 (Master Parisien de Recherche en Informatique), Paris, France.

    Introduction to cryptology: 3 hours (lecture), M2, École des Mines de Nancy, France.

    Training for "Informatique et Sciences du Numérique", Cryptology, Networks: 9 h, Université de Lorraine, Nancy, France. (Training for high school teachers who intend to teach this topic in high school).

- Marion Videau, teaching at the faculty of sciences, Université de Lorraine, Nancy, France:

    Introduction to algorithmic and programming: 40 hours (lectures and tutorial sessions), 20 hours (practical sessions), L1.

    Introduction to information system design: 10 hours (practical sessions), L3.

    Introduction to cryptography: 15 hours (lectures), 15 hours (tutorial sessions), M1.

    Introduction to information system security: 15 hours (lectures), 15 hours (tutorial sessions), M1.

    Supervision and jury of M2 students internships: 10 hours.

9.2.2. Internships

Cyril Bouvier, ENS Paris, "Integer Factoring on High-Performance Architectures", September 2011–August 2012, supervised by Paul Zimmermann.

Benjamin Dadoun, ENS Cachan, "Isolation of complex roots of univariate polynomials with the CEVAL algorithm", June–July 2012, supervised by Paul Zimmermann.

Nathan Lecoanet, ESIAL, "What speedup can we expect in the Number Field Sieve with non-linear polynomials?", June–July 2012, supervised by Paul Zimmermann.

Vlad-Cristian Miclea, Technical University of Cluj-Napoca (Romania), "Efficient FPGA implementation of finite-field multiplication algorithms", June 2012–September 2012, supervised by Jérémie Detrey.

Florent Noyer, ESIAL, "Parallel reconstruction of a polynomial from its roots", June–July 2012, supervised by Emmanuel Thomé

9.2.3. Supervision

HdR: Emmanuel Thomé, "Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques", Université de Lorraine, 13/12/2012, [1].

PhD in progress:

- Nicolas Estibals, "Algorithmes et arithmétique pour l'implémentation de couplages cryptographiques", started in 2009, co-supervised by Jérémie Detrey and Pierrick Gaudry.

- Răzvan Bărbulescu, "Number and function field sieve for discrete logarithm", started in 2011, supervised by Pierrick Gaudry.
- Hamza Jeljeli, "Using graphics accelerators for problems arising in the Number Field Sieve and Function Field Sieve algorithms", started in 2011, supervised by Jérémie Detrey and Emmanuel Thomé.
- Cyril Bouvier, "Integer Factoring on High-Performance Architectures", started in 2012, supervised by Paul Zimmermann.

9.2.4. *Juries*

- Paul Zimmermann was a member of the PhD thesis jury of Vincent Nivoliers (University of Lorraine), of the PhD thesis jury of Romain Lebreton (École Polytechnique), and of the "Habilitation à diriger des recherches" jury of Emmanuel Thomé (University of Lorraine).

9.3. Popularization

- With Nazim Fatès (MAIA project-team), Jérémie Detrey participated in a 2-hour television program dedicated to computer science and research, which was broadcast on the internal channel of the Nancy-Brabois children's hospital.
- Pierrick Gaudry:
  - co-organized a cycle of 3 conferences in the honour of Turing in Nancy. The three speakers were Giuseppe Longo, François Morain, and Jean Lassègue.
  - gave a talk at the "7ème colloque de l'ARCSI", in Metz for a general audience.
- Marion Videau:
  - participated to the film *Le Modèle Turing* of Catherine Bernstein (but her visual part was cut out during editing).
  - participated to a short television report for France 3 Lorraine about cryptography and her work as a researcher.
- Paul Zimmermann gave a 2-hour presentation about cryptography to students of "seconde" and "terminale" at the Lycée Jean de Pange in Sarreguemines.

CASCADE Project-Team

7. Dissemination

7.1. Editorial Boards

Editor-in-Chief

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

Associate Editor-in-Chief

–   of *Theory of Computing (ToC)*: Oded Regev

Associate Editor

–   of *Security and Communication Networks*: David Naccache

–   of *Journal of Cryptographic Design*: David Naccache

–   of *Encyclopedia of Cryptography and Security*: David Naccache

–   of *Journal of Small Scale Digital Device Forensics (publication currently on hold for financial reasons)*: David Naccache

–   of *Cryptologia* – Taylor & Francis: David Naccache

–   of *Information Processing Letters* – Elsevier: David Pointcheval

–   of *IEEE Transactions on Information Forensics and Security*: Michel Abdalla

Columnist (in charge of the bi-monthly CryptoCorner)

–   of the *IEEE Security and Privacy Magazine*: David Naccache

7.2. Program Committees

- RIVF – February 2012, Ho Chi Minh, Vietnam: David Naccache, Duong Hieu Phan
- TCC – March 2012, Taormina, Italy: Vadim Lyubashevsky
- EUROCRYPT – April 2012, Cambridge, UK: David Pointcheval (Program Chair)
- Pairing – May 2012, Cologne, Germany: Michel Abdalla (Program Chair), Damien Vergnaud
- STOC – May 2012, New York, NY, USA: Oded Regev
- AICT – May 2012, Stuttgart: David Naccache
- COSADE – May 2012, Darmstadt, Germany: David Naccache
- NTMS – May 2012, Istanbul, Turkey: David Naccache
- PKC – May, 2012, Darmstadt, Germany: Michel Abdalla, Vadim Lyubashevsky
- ACNS – June 2012, Singapore: Michel Abdalla
- HOST – June 2012, San Francisco, CA, USA: David Naccache
- ACISP – July 2012, Wollongong, Australia: Michel Abdalla
- Africacrypt – July 2012, Ifrane, Morocco: David Naccache
- ISCC – July 2012, Cappadocia, Turkey: David Naccache
- Secrypt – July 2012, Roma, Italy: David Naccache
- AReS – August 2012, Prague: David Naccache
- YACC – September 2012, Porquerolles, France: Michel Abdalla, Damien Vergnaud
- ProvSec – September 2012, Chengdu, China: Michel Abdalla, David Naccache

- ESORICS – September 2012, Pisa Italy: David Naccache
- Latincrypt – October 2012, Santiago, Chile: Michel Abdalla, Vadim Lyubashevsky
- IWSEC – November 2012, Fukuoka, Japan: Damien Vergnaud
- CARDIS – November 2012, Graz, Austria: David Naccache
- Intrust – December 2012, Egham, UK: David Naccache
- Indocrypt – December 2012, Kolkata, India: David Naccache
- CANS – December 2012, Darmstadt, Germany: Michel Abdalla

7.3. Teaching - Supervision - Juries

7.3.1. Teaching

Licence: David Naccache, Introduction to computer science, L1, Univ. Paris II

Licence: Maribel Fernandez, Formal languages, computability and complexity, ENS

Master: David Naccache, Scientific programming through practice, M1, ENS

Master: David Naccache, Jacques Stern, Damien Vergnaud, Introduction to Cryptology, M1, ENS

Master: Michel Abdalla, Vadim Lyubashevsky, Cryptography, M2, MPRI

Master: David Naccache, Computer Security, M2, Univ. Paris II

Master: David Naccache, Risk Management, M2, Univ. Paris II

Master: David Naccache, Computer forensics, M2, Univ. Paris II

Master: Duong-Hieu Phan, Provable Security, M2, Univ. Paris VIII

Master: David Pointcheval, Cryptography, M2, ESIEA

7.3.2. Supervision

PhD : Delphine Masgana Leresteux, *Injection de fautes et de logiciels sur les implémentations cryptographiques* Université Paris VII, 5 jul. 2012, Pierre-Alain Fouque

PhD : Olivier Blazy, *Preuves de connaissances interactives et non-interactives*, Université Paris VII, 27 sept. 2012, David Pointcheval

PhD : Roch Lescuyer, *Outils cryptographiques pour les accréditations anonymes*, Université Paris VII, 21 nov. 2012, David Pointcheval

PhD in progress: Mario Strefler, Diffusion chiffrée, 2009, David Pointcheval

PhD in progress: Viet Cuong Trinh, Traçage de traîtres et diffusion de données chiffrée, 2009, Duong Hieu Phan

PhD in progress: Léo Ducas, La cryptographie à base de réseaux, 2009, Phong Nguyen

PhD in progress: Aurore Guillevic, Étude de l'arithmétique des couplages sur des courbes algébriques pour la cryptographie, 2010, Damien Vergnaud

PhD in progress: Diana Maimut, Chiffrement pleinement homomorphe, 2011, David Naccache

PhD in progress: Eric Freyssinet, Modélisation de Botnets, 2011, David Naccache

PhD in progress: Tancrède Lepoint, La cryptographie à base de réseaux, 2011, Vadim Lyubashevsky

PhD in progress: Sylvain Ruhault, L'aléa en cryptographie, 2011, David Pointcheval & Damien Vergnaud

PhD in progress: Fabrice Ben Hamouda, La fuite d'information en cryptographie, 2012, Michel Abdalla & David Pointcheval

PhD in progress: Thomas Prest, La cryptographie à base de réseaux, 2012, Vadim Lyubashevsky & David Pointcheval

PhD in progress: Olivier Sanders, Externalisation de calculs cryptographiques, 2012, David Pointcheval

7.3.3. *Juries*

- HdR: Karthikeyan Bhargavan, *Towards the Automated Verification of Cryptographic Protocol Implementations*, Ecole Normale Supérieure, 4 may 2012: David Pointcheval
- HdR: Carlos Aguilar Melchor, *Sécurité, protection de la vie privée et cryptographie : quelques contributions*, Univ. Limoges, 26 jun. 2012: David Pointcheval (chair)
- HdR: Pascal Lafourcade, *Computer Aided Security for Cryptographic Primitives, Voting protocols, and Wireless Sensor Networks*, Univ. Grenoble, 6 nov. 2012: David Pointcheval (chair)
- PhD: Marion Daubignard, *Formal Methods for Concrete Security Proofs*, Univ. Grenoble, 12 jan. 2012: David Pointcheval (reviewer)
- PhD: Saeed Sedghi, *Towards Provably Secure Efficiently Searchable Encryption*, Univ. Twente, 17 feb. 2012: Michel Abdalla
- PhD: Avradip Mandal, *Provable Security and Indifferentiability* Univ. Luxembourg, 25 jun. 2012: David Pointcheval
- PhD: Delphine Masgana Leresteux, *Injection de fautes et de logiciels sur les implémentations cryptographiques*, Univ. Paris VII, 5 jul. 2012: David Pointcheval (co-advisor), David Naccache (chair)
- PhD: Adriana Suarez Corona, *Compilers and protocols for key establishment*, Univ. Oviedo, 24 jul. 2012: Michel Abdalla (Examiner)
- PhD: Olivier Blazy, *Preuves de connaissances interactives et non-interactives*, Univ. Paris VII, 27 sept. 2012: David Pointcheval (advisor), Michel Abdalla, Damien Vergnaud
- PhD: Anja Becker *La technique de représentation – Application à des problèmes difficiles en cryptographie* UVSQ, 26 oct. 2012: David Naccache (chair)
- PhD: Roch Lescuyer, *Outils cryptographiques pour les accréditations anonymes*, Univ. Paris VII, 21 nov. 2012: David Pointcheval (advisor), David Naccache (chair), Damien Vergnaud
- HdR: Bruno Robisson *Contribution à la sécurisation des composants vis-à-vis des attaques physiques* UMPC, 12 dec. 2012: David Naccache
- HdR: Olivier Ly *Un parcours de recherche des méthodes formelles aux robots humanoïdes* Univ. Bordeaux, 13 dec. 2012: David Naccache (reviewer)
- PhD: Amar Siad, *Protocoles de génération des clés pour le chiffrement basé sur de l'identité*, Univ. Paris 8, 17 dec. 2012: David Pointcheval, Duong-Hieu Phan
- PhD: Houssem Maghrebi *Masking Countermeasures against Higher-Order Side Channel Attacks: Security Evaluation and Enhancement by Specific Mask Encodings*, Telecom ParisTech, 21 dec. 2012: David Naccache
- HdR: Sylvain Guilley *Protection des Accélérateurs Matériels de Cryptographie Symétrique* TelecomParisTech, 20 dec. 2012: David Naccache

7.4. Invited Talks

7.4.1. *At Conferences*

- PKC 2012, Darmstadt, Germany (May): David Pointcheval
- NTCCS 2012, Oujda, Morocco (Avril): Damien Vergnaud
- LSFA 2012, Rio de Janeiro, Brazil (September): Maribel Fernandez
- ECC 2012, Queretaro, Mexico (October): Sorina Ionica
- ICCC 2012 Distinguished Lecturer, Paris (November): David Naccache

- ICISC 2012, Seoul Korea, (November): David Naccache
- CARDIS 2012, Graz (November): David Naccache
- SantaCrypt 2012, Prague (November): David Naccache

7.4.2. At Organized Schools

- Bar-Ilan Winter School on Cryptography. Ramat-Gan, Israel. February, 2012 : Vadim Lyubashevsky
- ECRYPT II Summer School on Lattices. Porto, Portugal. October, 2012 : Vadim Lyubashevsky

7.5. Scientific Animation

7.5.1. Organisation of Events

- ECRYPT II Summer School on Lattices, October 1 - 5, Porto Portugal: Michel Abdalla and Vadim Lyubashevsky
- a weekly seminar is organized: http://www.di.ens.fr/CryptoSeminaire.html

7.5.2. Steering Committees of International Conferences

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

7.5.3. Board of International Organizations

- Board of the *International Association for Cryptologic Research* (IACR): David Naccache (2010 – 2012), David Pointcheval (2008–2013)
- Scientific Board of the *Electronic Colloquium on Computational Complexity* (ECCC): Oded Regev

7.5.4. French Research Community

- Recruitment committee at Université Paris VII (PR 27): David Pointcheval
- Recruitment committee at Université of Lyon (PR 27): David Pointcheval
- Recruitment committee at Université de Caen (MC 25): Damien Vergnaud
- Recruitment committee at Université de Montpellier (MC 27): Damien Vergnaud
- Appointed member of the *Conseil National des Universités* (CNU): Damien Vergnaud

GALAAD Project-Team

8. Dissemination

8.1. Scientific Animation

Laurent Busé

- was a member of the program committee of the 2012 ISSAC international conference,
- is a member of the committee of "agrégation de mathématiques".

Evelyne Hubert

- is an associate editor of the Journal of Symbolic Computation (http://www.journals.elsevier.com/journal-of-symbolic-computation),
- is part of the Advisory Board of the MEGA conference series and co-edited this year a special issue of the Journal of Symbolic Computation,
- is part of the local Inria Committee for Invited Professors and Postodoctoral Fellows and was elected to the new hiring committee at the mathematics department of the University of Nice (CPRH 25-26-60).

Bernard Mourrain

- is an associate editor of the Journal of Symbolic Computation (http://www.journals.elsevier.com/journal-of-symbolic-computation),
- is member of the Advisory Board of the MEGA conference series,
- is chair of the local Inria Committee for Courses and Conferences.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Laurent Busé teaching activities:

> Master : *Courbes et Surfaces*, 42h ETD, first year of Master MAM4 of the EPU, University of Nice.
>
> Master MDFI: *Elimination theory*, 13h, University of Luminy, Marseille.

Mathieu Collowald teaching activities:

> L1 MASS : Statistics (Exercices), 20h, University of Nice-Sophia Antipolis.
>
> L1 I : Algebra (Exercices), 44h, University of Nice-Sophia Antipolis.

André Galligo teaching activities:

> Master : *Introduction to random polynomials and matrices*, University of Buenos Aires, Argentina, 20h.

Bernard Mourrain teaching activities:

> Master 2: *Computational Algebra for Real Geometry* 30h ETD, Master 2 of Mathematics, Lab. J.A. Dieudonné.
>
> Master MDFI: *Elimination theory*, 15h, University of Luminy, Marseille.

8.2.2. Supervision

8.2.2.1. Defended Habilitation thesis

Evelyne Hubert was awarded her habilitation in mathematics from the University of Nice in September 2012. The Jury consisted of Elizabeth Mansfield (University of Kent, UK), Michael Singer (North Carolina State University, USA), Emilio Musso (Politecnico de Turino, Italy), Pascal Chossat (University of Nice), Bruno Salvy (Inria Paris), Bernard Mourrain (Inria Méditerranée).

8.2.2.2. Ph.D. thesis in progress

Marta Abril Bucero, Moment matrices, real algebraic geometry and polynomial optimization. Advisor: Bernard Mourrain.

Mathieu Collowald, Integral representation of shapes for feature conservation or extraction. Advisors: Evelyne Hubert and Bernard Mourrain.

Abdallah Lachaal, Geometric computing with procedural models and applications. Advisor: Bernard Mourrain.

8.2.2.3. Internship

Valentin Michelet, *Intersection courbe/surface au moyen des représentations matricielles* , 3 months, Master1.

Baptiste Mourrain, *A dynamic web application*, 1 month, first year of engineer school.

Zora Abdoul Kaid, *Isoparametrisation of multi-patch surfaces*, 3 months, MAM4, Master1.

Rémy Abdeljalil, *Adaptative approximation of point sets by T-splines surfaces*, 3 months, MAM4, Master1.

8.2.3. Juries

Bernard Mourrain was member of the HDR of Evelyne Hubert, of the Ph.D. committee of R. Lebreton "Contribution à l'algorithmique détendue et à la résolution des systèmes polynomiaux", École Polytechnique (11/12/2012), of the PhD of C. Preusakarn "Reconstructing of Plant Architecture from 3D Laser Scanner Data", University of Montepellier 2, (19/12/2012).

André Galligo was a member of the PhD of Santiago Laplagne, "Algoritmos de Algebra Conmutativa en Anillos de Polinomios" University of Buenos Aires (Argentina), Avpil 2012, of the PhD of Nelly Villamizar, "Algebraic Geometry of Splines". University of Oslo (Norway), December 2012.

<p align="center">**GEOMETRICA Project-Team**</p>

8. Dissemination

8.1. Animation of the scientific community

8.1.1. Editorial boards of scientific journals

P. Alliez is an associate editor of *ACM Transactions on Graphics* and *Graphical Models*.

J-D. Boissonnat is a member of the editorial board of the *Journal of the ACM*, *Discrete and Computational Geometry*, *Algorithmica*, the *International Journal of Computational Geometry and Applications* and the electronic *Journal of Computational Geometry*. He is also a member of the editorial advisory board of the Springer Verlag book series *Geometry and Computing*.

F. Chazal is an associate editor of *Graphical Models* and *SIAM journal on Imaging Science*.

S. Oudot is co-editor with T. Dey of the special issue of *Discrete and Computational Geometry* on SoCG 2012.

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

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

M. Yvinec is a member of the editorial board of *Journal of Discrete Algorithms*.

P. Alliez, M. Teillaud (review manager until April 30th), and M. Yvinec are members of the CGAL editorial board.

8.1.2. Conference program committees

Pierre Alliez was a program committee member of EUROGRAPHICS main conference, EUROGRAPHICS Symposium on Geometry Processing and International Workshop on Point Cloud Processing (a CVPR workshop).

Steve Oudot was a program committee member of SoCG 2012 (ACM Symposium on Computational Geometry).

Frédéric Chazal was a program committee member of ATMCS 2012 (5th conf. on Algebra and Topology: Methods, Computation and Science), SMAI-SIGMA 2012 conference, SMAI-MAIRCI workshop 2012, ICPRAM 2012 and 2013 (International Conference on Patern Recognition Applications and Methods).

Frédéric Chazal is a program committee member of SoCG 2013 (ACM Symposium on Computational Geometry).

David Cohen-Steiner was a program committee member of the EUROGRAPHICS Symposium on Geometry Processing.

J-D. Boissonnat was a program committee member of "Mathematical Methods for Curves and Surfaces", Geometric Modeling and processing (GMP 2012), EUROGRAPHICS Symposium on Geometry Processing (SGP 2012)

Florent Lafarge was program chair of IEEE CVPR workshop on Point Cloud Processing and a program committee member of EUROGRAPHICS short papers and ISPRS congress.

8.1.3. Steering committees

Monique Teillaud is a member of the Computational Geometry Steering Committee.

8.1.4. Ph.D. thesis and HDR committees

Pierre Alliez was a referee and member of the Ph.D. defense committee of Nicolas Mellado (Inria Bordeaux) and David Bommes (RWTH Aachen).

Steve Oudot was a member of the Ph.D. defense committee of Arijit Ghosh (Inria Sophia-Antipolis).

Jean-Daniel Boissonnat was a member of the HDR defense of Eric Colin de Verdière (ENS Ulm)

Olivier Devillers was a member of the Ph.D. defense committee of Daniela Maftuleac (Univ. Marseille)

8.1.5. *Inria committees*

F. Chazal is the chair of the "Commission scientifique" at Inria Saclay - île de France.

Monique Teillaud is a member of the Inria Evaluation Committee.

She coordinated the working group on life of software of the evaluation committee. She is a member of the working group on the Inria software database (BIL).

She was a member of the national Inria CR2 and DR2 recruitment committees, as well as a member of the Inria Starting and Advanced Research Positions committees.

She is also a member of both Inria Sophia CDT (Committee for Technologic Development) and Inria national CDT.

Florent Lafarge is a member of the comité de Suivi Doctoral (CSD) of Inria Sophia.

Pierre Alliez is a member of the comité de médiation scientifique of Inria Sophia Antipolis - Mediterranee.

8.1.6. *Other committees*

J.-D. Boissonnat is a member of the working groups GP1 (Modèles et calcul) and GP2 (Logiciels et systèmes informatiques) de l'Alliance des sciences et technologies du numérique (Allistène).

J.-D. Boissonnat is a member of the AERES Board (Evaluation Agency for Research and Higher Education).

J-D. Boissonnat chaired the Visiting Committee of the Geometric Modeling and Scientific Visualization Center of the King Abdullah University of Science and Technology (KAUST, Saudi Arabia, 2012).

J-D. Boissonnat chaired the recruitment committee of ENS Lyon (PU n°4037 / CS 27)

F. Chazal is a member of the Scientific Council of AMIES (Agence pour les Mathématiques en Interaction avec l'Industrie et la Société)

F. Chazal is a member of the "Comité de pilotage" of the MAIRCI and SIGMA (ex-AFA) groups of the SMAI.

F. Chazal is a member of the "Bureau du Comité des Projets" at Inria Saclay.

M. Glisse is a member of the experts group of AFNOR for the standardization of the C++ language within the ISO/WG21 working group.

M. Teillaud was a member of the LIAMA Visiting Committee.

8.1.7. *Conference organization*

J.-D. Boissonnat chairs the scientific committee of the Jacques Morgenstern Colloquium.

Monique Teillaud organized the *Minisymposium on publicly available geometric/topological software* (with Menelaos Karavelas), Chapel Hill, USA, June 17&19, 2012.

Monique Teillaud was a member of the scientific committee of the workshop SIGMA'2012: Signal, Image, Geometry, Modelling, Approximation, Marseille, November 19-23.

CGAL developers meeting, Inria, December 17-21.

8.1.8. *Web site*

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

8.2. Teaching

We give here the details of courses. Web pages of the graduate courses can be found on the web site :
http://www.inria.fr/sophia/geometrica/

Traitement numérique de la géométrie, Lorsque nos maths s'incarnent dans les ordinateurs, Monique Teillaud, 3h, Centre de Formation d'Apprentis de l'Industrie, Avignon.

"à quoi sert un triangle ?", Monique Teillaud, 2x2h, Collège Le Prés des Roures, Le Rouret, in the framework of the national Week of Mathematics.

Master: Computational Geometry: from Theory to Applications, Steve Oudot, 20h ETD, M1, École Polytechnique.

Master: Géométrie algorithmique, Olivier Devillers, 13h ETD (2011-2012) 24h ETD (2012-2013), M1, Université de Nice.

Master: Algorithmes géométriques: théorie et pratique, Pierre Alliez, Olivier Devillers, and Monique Teillaud, 28h ETD, M2, Université de Nice.

Master: Computational Geometry Learning, J.-D. Boissonnat, F. Chazal and M. Yvinec, 25h, M2, MPRI (Paris).

Master: Computational Geometry: from Theory to Applications, S. Oudot, 20h, M1, école Polytechnique.

Master: Maillages 3D et applications, P. Alliez, 21h, Ecole des Ponts ParisTech (Paris).

Master: Mathématiques pour la géométrie, P. Alliez, 24h, EFREI (Ecole d'Ingénieur des Technologies de l'Information et de la Communication, Paris).

Doctorat: Geometric Inference, F. Chazal and D. Cohen-Steiner, 20h, Université Paris Sud (Orsay).

Master: Markov Random Fields, F. Lafarge, 9h, EPU Sophia Antipolis.

Master: Image segmentation, F. Lafarge, 11h, University of Nice Sophia Antipolis.

Doctorat: Introduction to Geometric Inference, F. Chazal, 3h, Neuchâtel University.

8.2.1. Ph.D. theses

Arijit Ghosh, Piecewise Linear Reconstruction and Meshing of Submanifolds of Euclidean Space, Université de Nice-Sophia Antipolis, May 30, 2012, J-D. Boissonnat.

Bertrand Pellenard, Generation of quadrangle meshes. Université de Nice-Sophia Antipolis, Dec 18, 2012, P. Alliez.

Claire Caillerie, Sélection de modèles pour l'inférence géométrique, Université Paris XI, started September 2008, Frédéric Chazal and Pascal Massart (in progress).

Alexandre Bos, Topological methods for geometric data classification, Université Paris XI, started September 2010, Frédéric Chazal and Steve Oudot (in progress).

Mikhail Bogdanov, Triangulations in non-Euclidean spaces, started October 1st 2010, Monique Teillaud (in progress).

Yannick Verdié, Urban scene analysis from unstructured point data, Université de Nice-Sophia Antipolis, started November 2010, Florent Lafarge (in progress).

Mickael Buchet, Topological and geometric inference from measures, Université Paris XI, started October 2011, Frédéric Chazal and Steve Oudot (in progress).

Ross Hemsley, Probabilistic methods for the efficiency of geometric structures and algorithms, started October 1st 2011, Olivier Devillers (in progress).

Clément Maria, Data structures for simplicial complexes, Université de Nice-Sophia Antipolis, started October 1, 2011, J-D. Boissonnat (in progress).

Simon Giraudot, Robust Shape Reconstruction, Université de Nice-Sophia Antipolis, started November 2011, Pierre Alliez (in progress).

Xavier Rolland-Névière, Robust watermarking of 3D Shape, Université de Nice-Sophia Antipolis, started November 2011, Pierre Alliez and Gwenael Doerr from Technicolor (in progress).

Sven Oesau, Reconstruction of indoor scenes, Université de Nice-Sophia Antipolis, started April 2012, Pierre Alliez and Florent Lafarge (in progress).

Manish Mandad, Robust Shape Approximation, Université de Nice-Sophia Antipolis, started November 2012, Pierre Alliez (in progress).

Rémy Thomasse, Smoothed complexity of geometric structures and algorithms, started December 1st 2012, Olivier Devillers (in progress).

8.2.2. Internships

Internship proposals can be found on the web at http://www.inria.fr/sophia/geometrica/

Manish Mandad, Shape approximation with guarantees, Master CBB (France).

Mathier Schmitt, Meshing of the hyperbolic octagon, L3 ENS Lyon (Monique Teillaud).

Claudia Werner, Triangulations on the sphere, Hochschule für Technik Stuttgart (Monique Teillaud)

8.3. Participation to conferences, seminars, invitations

8.3.1. Invited Talks

Frédéric Chazal, "Topological Data Analysis using distance based functions", 4th International Workshop on computational Topology in Image context, Bertinoro, Italy, february 2012.

Olivier Devillers, "EuroCG-2012", Delaunay triangulation, theory vs practice, March 19th.

Pierre Alliez, "Robust Shape Reconstruction", Dive with an Expert Seminar, Schlumberger Montpellier Technology Center, May 2012.

J-D. Boissonnat, "Aspects algorithmiques de la triangulation des variétés", Colloque Mathématiques et Formation des Ingénieurs", Coetquidan, Juin 2012.

Frédéric Chazal, "Topological Data Analysis using distance based functions", Dynamics, Topology and Computations (DyToComp 2012 - satellite conference of 6th European Congress of Mathematics), Bedlewo Poland, June 2012.

Frédéric Chazal, "Detection and Approximation of Linear Structures in Metric Spaces" Workshop on Algorithms for Modern Massive Data Sets (MMDS 2012), Stanford USA, July 2012.

J-D. Boissonnat, "Delaunay-type structures for manifolds", Workshop on Applied and Computational Topology (ATMCS), Edinburgh July 2012.

Pierre Alliez, "Advances in Architectural Geometry", Paris, September.

Pierre Alliez, "MICCAI workshop on Mesh Processing in Medical Image Analysis", Nice, October.

Pierre Alliez, "3DIMPVT: 3D Imaging, Modeling, Processing, Visualization and Transmission", Zurich, October.

J-D. Boissonnat, "Provably good meshes", Dive with an Expert Seminar, Schlumberger Montpellier Technology Center, October 2012.

Frédéric Chazal, "Persistence Stability for Geometric complexes" , Workshop on Algebraic Topology and Machine Learning, NIPS 2012, Lake Tahoe USA, December 2012.

8.3.2. Seminars

Members of the project have presented their published articles at conferences. The reader can refer to the bibliography to obtain the corresponding list. We list below all other talks given in seminars, summer schools and other workshops.

Olivier Devillers, «Constructions incrémentielles randomisées», journées Présage, january 12-13.

Marc Glisse, «Complexité moyenne et Visibilité 3D», journées Présage, january 12-13.

Olivier Devillers, Olivier Devillers, «Delaunay triangulations, theory vs. practice», journées de géometrie algorithmique, april 2-6.

Clément Maria, "A Data Structure to Represent Simplicial Complexes", journées de géométrie algorithmique, april 2-6.

Ross Hemsley, "Pivot Walk - A Faster Walking Strategy for Point Location" , journées de géométrie algorithmique, april 2-6.

Ramsay Dyer, "Stability of Delaunay-type structures for manifolds", journées de géométrie algorithmique, april 2-6.

Frédéric Chazal, "Geometric Inference using distance-like functions", Minisymposium on Computational Geometric Learning, Exploring geometric structures in high dimensions, CG:APT, SoCG 2012.

Frédéric Chazal, "Persistence Stability for Geometric complexes", Workshop on Topological data analysis and machine learning theory, Banff Canada, October 2012.

Olivier Devillers, «Hypergraphes de régions vides I : point de vue de la géométrie algorithmique», journées Présage, october 18-19.

Marc Glisse, «Complexité moyenne en visibilité, sans les logs», journées Présage, october 18-19.

Frédéric Chazal, "Detection and Approximation of Linear Structures in Metric Spaces", SMAI-SIGMA Conference 2012, CIRM Luminy France, November 2012.

Ramsay Dyer, "Stability of Delaunay-type structures for manifolds", SMAI-SIGMA Conference 2012, CIRM

Clément Maria, "A space and time efficient implementation for computing persistent homology", Computational Geometric Learning Workshop, Berlin, december 2012.

Pierre Alliez, "The CGAL Library and Mesh Generation", Graduate school of the EUROGRAPHICS Symposium on Geometry Processing, July 2012.

8.3.3. *The Geometrica seminar*
http://www.inria.fr/sophia/geometrica/
The GEOMETRICA seminar featured presentations from the following visiting scientists:

Xianhai Meng (Beihang University, China): Mesh Generation and 3D Geological Modeling.

Thijs van Lankveld (University of Utrecht). Reconstructing urban geometry per surface from point samples. March 19.

Vincent Vidal (LIRIS, Lyon, France). Modèles graphiques pour segmenter et remailler les maillages surfaciques triangulaires. April 11.

Mark Blome (Konrad-Zuse-Zentrum für Informationstechnik, Berlin). Modeling of complex 3D nano-photonic devices using Computer Aided Design techniques. July 3.

Benjamin Burton (University of Queensland, Australia). Unknot recognition and the elusive polynomial time algorithm. October 3.

8.3.4. *Scientific visits*

Clément Maria visited Pr. Coutsias (University of New Mexico) for one week in september and Pr. Dey (Ohio State University) for one week.

Pierre Alliez, RWTH Aachen, October 10-12.

Olivier Devillers, EPI RAP, November 19-21.

Ross Hemsley, EPI RAP, November 19-21.

Florent Lafarge, University of Auckland, December 17- January 11.

GRACE Team

8. Dissemination

8.1. Scientific Animation

- D. Augot is editor for the journal "RAIRO - Theoretical Informatics and Applications"
- D. Augot was editor of a special issue of Designs, Codes and Cryptography.
- D. Augot is co-organizer, with P. Loidreau, of the French CCA (Coding, Cryptography and Algorithms) seminar, http://cca.saclay.inria.fr, held in Paris three times per year.
- D. Augot was in the program committee of YACC 2012, Porquerolles.
- D. Augot was a reviewer for IEEE Transactions on Information Theory, Designs, Codes and Cryptography, SIAM Journal on Discrete Mathematics, Journal of Symbolic Computation, AAECC.
- B. Smith was a reviewer for ANTS, Eurocrypt, Asiacrypt, PQCrypto, RAIRO ITA, ETRI Journal.
- B. Smith contributes to the American Mathematical Society's Mathematical Reviews (MathSciNet).
- A. Zeh was reviewer for Advances in Mathematics of Communications (AMC), IEEE Communications Letters and IEEE Transactions on Information Theory.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master MPRI : Daniel Augot, Error correcting codes and applications to cryptography, 24, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. Paris Sud, U. P. et M. Curie, France.

Master MPRI : F. Morain, arithmetic algorithms for cryptology, 9h, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. Paris Sud, U. P. et M. Curie, France.

Master MPRI: B. Smith, arithmetic algorithms for cryptology, 12h, M2, U. Paris Diderot, ENS Ulm, ENS Cachan, Polytechnique, U. ParisSud, U. P. et M. Curie, France

Master : F. Morain, 9 lectures of 1.5h, 3rd year course "cryptology" at École polytechnique (M1).

Master: B. Smith, 10 practical classes of 2h, 3rd year course "cryptology" at École polytechnique (M1).

Licence : F. Morain, 10 lectures of 1.5h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique (L2).

Licence: B. Smith, 20 TDs of 2h, 1st year course "Introduction à l'informatique" (INF311) at École polytechnique (L2).

Licence: A. Couvreur, 4 TP's of 2h on Matlab Programming for 1st year students at École Polytechnique (L2).

8.2.2. Supervision

PhD: Guillaume QUINTIN, "Sur l'algorithme de d'ecodage en liste de Guruswami–Sudan sur les anneaux finis", École polytechnique, defended 2012/11/22.

PhD in progress : Cécile GONÇALVES, Advanced cardinality algorithms for cryptographically interesting curves, 01/10/2011, F. Morain and B. Smith

8.2.3. Juries

- D. Augot was an examiner in the jury of Julia Pieltant, "Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis", Université d'Aix-Marseille, December 12 2012.

- D. Augot was an examiner in the jury of Guillaume Quintin, "Sur l'algorithme de décodage en liste de Guruswami-Sudan sur les anneaux finis", école Polytechnique, November 22 2012.

- D. Augot was an examiner in the jury of Anja Becker, "La technique de représentation – Application à des problèmes difficiles en cryptographie", UVSQ, October 26 2012.

- D. Augot was an examiner in the jury of Amar Siad, "Protocoles de génération des clés pour le chiffrement basé sur de l'identité", Université Paris 8, December 21 2012.

- F. Morain was president of the jury of Stéphane Jacob, Mars 08 2012 (Protection cryptographique des bases de données: conception et cryptanalyse).

- B. Smith was an examiner in the jury of Jean-Pierre Flori, "Fonctions booléennes, courbes algébriques et multiplication complexe", Télécom ParisTech, February 3 2012.

8.3. Popularization

- D. Augot made a presentation in the high school at Courcouronnes "Quand $1 \oplus 1 = 0$".

- D. Augot was interviewed by French novelist François Bon.

- F. Morain gave a talk on "Turing et la cryptanalyse", during the special days for the centenary of the birth of Turing, Nancy 2012/09/20.

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

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorships

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

H. Cohen is an editorial board member of *Journal de Théorie des Nombres de Bordeaux*; he is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM)*.

J.-M. Couveignes is associate editor of *Séminaires et Congrès* since 2008, of *Mathematics of Computation* since 2008, of *London Mathematical Society Journal for Computation and Mathematics* since 2009 and of *Publications mathématiques de Besançon* since 2010.

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

9.1.2. Invited talks

- A. Enge: "Class polynomials for abelian surfaces by complex approximations" at *Number Theory, Discrete Mathematics and Their Applications*, Tsinghua University, China, 25–27/05

9.1.3. Conference organisation and programme committees

A. Enge acts on the scientific advisory board of the *Journées Nationales de Calcul Formel.*

9.1.4. Seminar

The following external speakers have given a presentation at the LFANT seminar, see
http://lfant.math.u-bordeaux1.fr/index.php?category=seminar

- Charles Boyd (Amherst): "Paridroid"
- Loïc Grenié (Bergamo): "A modular HNF", "bnfinit ()"
- Vassily Golyshev (Bonn): "Searching for congruences of Galois representations "
- Marco Streng (Warwick): "Smaller class invariants for quartic CM-fields"
- Gaëtan Bisson (Sydney): "Un algorithme à la Pollard pour le problème du sac à dos"
- Bruno Salvy: "Itération de Newton: du numérique à la combinatoire, et réciproquement"
- Bernhardt Schmidt (Singapore): "Values and ideals in combinatorial problems"
- Fernando Mario (Berlin): "Packings of bodies in Euclidean space"
- Luca De Feo (Versailles): "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

9.1.5. Research administration

K. Belabas is the head of the mathematics department of University Bordeaux 1. He also leads the computer science support service ("cellule informatique") of the Institute of Mathematics of Bordeaux and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

He is a permanent invited member of the councils of both the math and computer science department (UFR) and the Math Institute (IMB).

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

Since January 2011, J.-M. Couveignes is involved in the *GDR mathématiques et entreprises* and in the *Agence pour les mathématiques en interaction avec l'entreprise et la société*.

A. Enge is responsible for the international affairs of Inria–Bordeaux-Sud-Ouest and a member of the COST-GTRI, the Inria body responsible for evaluating international partnerships.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- K. Belabas

    Algèbre et Calcul Formel, 100h, M2, Université Bordeaux 1, France
- J.-P. Cerri

    Cryptographie et Arithmétique, 24h, L3, Université Bordeaux 1, France

    Arithmétique, 36h, M1, Université Bordeaux 1, France

    Algorithmic Number Theory, 70h, M2, Université Bordeaux 1, France
- J.-M. Couveignes

    Algorithms for public key cryptograph, 40h, M2, Université Bordeaux 1, France

    Algorithms for number fields, 40h, M2, Université Bordeaux 1, France

    Algorithms for Modular Curves, Jacobians and Forms, 16h, Tsinghua University, Beijing, China
- A. Enge:

    Elliptic Curves in Cryptologie, 14h, L2–PhD, Tsinghua University, Beijing, China
- P. Lezowski: Moniteur and ATER at Université Bordeaux 1

    MHT411: Groupes, anneaux, corps, TD, 40h, L2, Université Bordeaux 1, France

    M1MI1002: Fondamentaux pour les Mathématiques et l'Informatique, cours–TD, 80h, L1, Université Bordeaux 1, France
- N. Mascot: Moniteur at Université Bordeaux 1

    MOSE1003: Analyse et algèbre, cours–TD, 36h h, L1, Université Bordeaux 1, France

    M1MI1001: Bases de l'analyse, cours–TD, 37.5h, L1, Université Bordeaux 1, France
- A. Page: Moniteur at Université Bordeaux 1

    M1CP3022:Maths analyse II, TD, 42h, L2, Université Bordeaux 1, France

    M1mi2012:Algèbre 1, TD, 18h, L1, Université Bordeaux 1, France

9.2.2. Supervision

- K. Belabas, A. Enge

    PhD Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, University Bordeaux
- K. Belabas, J.-M. Couveignes

    PhD Nicolas Mascot, *Calcul de représentations galoisiennes modulaires*, University Bordeaux
- K. Belabas, P. Stevenhagen

    PhD Athanasios Angelakis, *Number fields sharing the same abelianized Galois group*, ALGANT, University Bordeaux and University Leiden

    K. Belabas, T. Dokchitser, P. Stevenhagen

    PhD Julio Brau, *Computing Galois representations attached to elliptic curves*, ALGANT, University Bordeaux and University Leiden

- A. Enge, D. Robert

    PhD Enea Milio, *Isogénies entre surfaces abéliennes*, University Bordeaux

9.2.3. *Juries*

- K. Belabas

    PhD Pierre Lezowski, *Questions d'Euclidianité*, University Bordeaux, 07/12 (committee).

    HdR Emmanuel Thomé *Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques*, University Nancy-Lorraine, 13/12 (referee, committee).

- A. Enge

    PhD Jean-Pierre Flori, *Fonctions booléennes, courbes algébriques et multiplication complexe*, Télécom Paristech, 03/02 (president)

    PhD Aurélien Bajolet, *Aspects numériques de l'analyse diophantienne*, University Bordeaux, 07/12 (committee)

9.3. Popularization

N. Mascot and A. Page have given a presentation "Cryptologie" for the Fête de la Science.

J.-M. Couveignes has given a presentation at the seminar "Unithé ou café" of INRIA Bordeaux–Sud-Ouest on "Vous trouvez ça complexe? Tant mieux!".

A. Enge has contributed to the Inria exhibition around Turing, computing machines and cryptology for the Fête de la Science.

A. Enge has given a presentation "Petit théorème de Fermat et courbes elliptiques, les mathématiques au service du secret" for the yearly meeting of Association des professeurs de mathématiques de l'enseignement public.

POLSYS Project-Team

9. Dissemination

9.1. Scientific Animation

Elias Tsigaridas visited the Computer Science Department of Aarhus University, Denmark (28 May - 3 June) and gave a talk on random polynomials. He participated in ISSAC 2012 (July 22-25, 2012) in Grenoble, France and gave a talk on real solving polynomials with coefficients in multiple extension fields. He visited (23 Oct – 4 Noe) the Chinese Academy of Sciences, Beijing, China, as an invited speaker for the workshop Computational Geometry of the Asian Symposium on Computer Mathematics (ASCM), where he gave a talk on "Univariate Real Root Isolation in Extension Field and Applications to Topology of Curves". During his stay in China, he was also invited to give a talk at Institute of Software of the State Key Lab of Computer Science, about random polynomials. He was invited at the Department of Applied Mathematics, Univ. of Crete, Greece (15 Jun – 2 Jul) and gave a talk at the department's seminar about random polynomials. He participated and gave a talk in 7th Athens Colloquium on Algorithms and Complexity (ACAC) in Athens, Greece (27–28 July) on solving polynomials with coefficients on an extension field. He participated in the conference Computer Algebra in Scientific Computing (CASC) that was held in September 3 - 6, at Maribor, Slovenia. He visited in the North Carolina State University, USA (15 – 20 Oct) where he gave a talk at the Department's Symbolic Computation seminar with title "Real algebraic geometry and stochastic games". He participated in the Mathematics, Algorithms and Proofs 2012 (MAP) workshop of the GEOLMI ANR project (Univ. Konstanz, Germany, September 17 - September 21, 2012). Finally, he was invited to give a talk in the X-mas seminar of the ERGA lab of the Dept. of Informatics, Univ. of Athes, Greeece (27 December 2012) on real solving polynomials in the presence of logarithms.

J.C. Faugère was invited to give an invited talk in the international workshop on efficient linear algebra for Gröbner basis computation in Kaiserslautern. J.C. Faugère visited the Mathematics Department of the North Carolina State University and give a talk at the Computer Science Department of Duke University (USA). J.-C. Faugère, is member of the MEGA Advisory Board.

D. Wang is member of the editorial board of:

- Editor-in-Chief and Managing Editor for the journal "Mathematics in Computer Science" (published by Birkhäuser/Springer, Basel).
- Executive Associate Editor-in-Chief for the journal "SCIENCE CHINA Information Sciences" (published by Science China Press, Beijing and Springer, Berlin).
- Member of the Editorial Boards for the
    - Journal of Symbolic Computation (published by Academic Press/Elsevier, London),
    - Frontiers of Computer Science in China (published by Higher Education Press, Beijing and Springer, Berlin),
    - Texts and Monographs in Symbolic Computation (published by Springer, Wien New York),
    - Book Series on Mathematics Mechanization (published by Science Press, Beijing),
    - Book Series on Fundamentals of Information Science and Technology (published by Science Press, Beijing).
- Editor for the Book Series in Computational Science (published by Tsinghua University Press, Beijing).

L. Perret co-organized with C. Cid the Ecrypt II Summer School on Tools (Mykonos, Greece, 28 May - 1 June 2012 https://www.cosic.esat.kuleuven.be/ecrypt/courses/mykonos12/).

J.-C Faugère, and G. Renault delivered an invited talk at the Ecrypt II Summer School on Tools (Mykonos, Greece, 28 May - 1 June 2012 https://www.cosic.esat.kuleuven.be/ecrypt/courses/mykonos12/).

J.-C Faugère was the programm chair of third international conference on Symbolic Computation and Cryptography (SCC 2012) (International Centre for Mathematical meetings (CIEM), Castro Urdiales, 11-13 July 2012, http://scc2012.unican.es/).

L. Perret was in the programm comittee of SCC'12.

J.-C Faugère and L. Perret were in P.C. of the YACC'12 conference (September 24 – September 28, 2012, Porquerolles Island, France, http://yacc.univ-tln.fr/category/yacc-2012/).

L. Perret was in the programm comittee of International Conference on Practice and Theory in Public-Key Cryptography (PKC'2013) (Nara, Japan, February 26 - March 1, 2013, http://ohta-lab.jp/pkc2013/

J.-C Faugère and L. Perret are in the programm comittee of Symbolic Computations and Post-Quantum Cryptography Online Seminar organised by the Stevens Institute (USA, http://www.stevens.edu/algebraic/SCPQ/)

J.-C Faugère and L. Perret are guest editors of a Special issue of Journal of Symbolic Computation on "Mathematical and Computer Algebra Techniques in Cryptology" (in progress)

M. Safey El Din is member of the editorial board of Journal of Symbolic Computation. He was member of the Programm committee of CASC 2012. He visited the department of Computer Science at the Univ. of Western Ontario in February 2012 and Sept. 2012. With J.-C. Faugère, L. Perret and E. Tsigaridas, he visited the Symbolic Computation Group at North Carolina State University in October 2012. He was member of the National Council of Universities until Sept. 2012. Since Nov. 2012, he is the head of the Scientific Computing Department of LIP6. He has been nominated at the Institut Universitaire de France.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master : Ludovic Perret, Introduction à la Sécurité, 140 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Modeling and numerical and symbolical resolutions of problems via MAPLE and MATLAB systems, 14 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : J. Berthomieu, Linear Algebra and Applications, 35 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, Algèbre Linéaire et Applications, 35 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, Cryptologie Appliquée, 70 heures équivalent TD, niveau M2, Univ. Pierre-et-Marie-Curie, France

Master : Guénaël Renault, co-head of the speciality on"Sécurité, Fiabilité et Performance Numérique" in the Computer Science Master Program, niveaux M1-M2, Univ. Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Modeling and numerical and symbolical resolutions of problems via MAPLE and MATLAB systems, 21 heures équivalent TD, niveau M1, Univ. Pierre-et-Marie-Curie, France

Master : M. Safey El Din, Polynomial Systems, Computer Algebra and Applications, 17 heures équivalent TD, niveau M2, Master Parisien de Recherche en Informatique, France

9.2.2. Supervision

PhD : Christopher Goyet, Cryptanalyse algébrique par canaux auxiliaires, Univ. Pierre-et-Marie-Curie, 7 novembre 2012, J.-C. Faugère, G. Renault

PhD : Pierre-Jean Spaenlehauer, Résolution de systèmes multi-homogènes et déterminantiels: algorithmes, complexités et applications, Univ. Pierre-et-Marie-Curie, 9 octobre 2012, J.-C. Faugère, M. Safey El Din

PhD in progress : Jules Svartz, Solving polynomial systems with symmetries, inscription octobre 2011, J.-C. Faugère

PhD in progress : Louise Huot, Étude des systèmes polynomiaux en cryptologie sur les courbes, Univ. Pierre-et-Marie-Curie, inscription octobre 2010, J.-C. Faugère, G. Renault

PhD in progress : Rina Zeitoun, Cryptologie sur cartes a puces et methodes algebriques, Univ. Pierre-et-Marie-Curie, inscription mars 2012, J.-C. Faugère, G. Renault

PhD in progress : Frederic Urvoy de Portzamparc, Cryptanalyse algébrique et étude de la sécurisation contre les attaques physiques des primitives fondées sur la théorie des codes, inscription février 2012, J.-C. Faugère, L. Perret

PhD in progress : Simone Naldi, Algorithmes de la géométrie algébrique réelle pour la théorie du contrôle, Univ. Paul Sabatier (Toulouse), inscription octobre 2012, D. Henrion, M. Safey El Din

9.2.3. *Juries*

J.-C. Faugère was member of 4 committees: 3 Prof. (UPMC, Montpellier, Rouen) and 1 MdC (UPMC).

9.3. Popularization

J.-C. Faugère gives a talk at Dassault Systèmes on applications of Gröbner Bases to industrial problems.

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

8. Dissemination

8.1. Scientific Animation

8.1.1. Editorial activities.

- *IEEE Transactions on Information Theory*, associate editor: J.-P. Tillich for *Coding Theory*.
- *Designs, Codes and Cryptography*, associate editor: P. Charpin, since 2003.
- *RAIRO - Theoretical Informatics and Applications*, associate editor: N. Sendrier.
- Special issue in Coding and Cryptography, *Designs, Codes and Cryptography*, 2012, co-editor: A. Canteaut.
- *FSE 2012 (Fast Software Encryption)*: March, 19-21, 2012, Washington DC, USA, Program chair and editor of the proceedings: A. Canteaut
- *Finite Fields and Their Applications. Character Sums and Polynomials*, Radon Series on Computational and Applied Mathematics, Degruyter, In Press. Editeurs: P. Charpin, A. Pott (U. Magdeburg) et A. Winterhof (Austrian Acad. of Sc.)
- A. Canteaut is a member of the steering committee of *Fast Software Encryption (FSE)*;
- N. Sendrier is a member of the steering committee of *Post-quantum cryptography (PQCrypto)*.

8.1.2. Program committees

- FSE 2012: March 19-21, 2012, Washington DC, USA (A. Canteaut, program chair);
- PKC 2012: May 21-23, 2012, Darmstadt, Germany (N. Sendrier);
- SETA 2012, June 4-8, 2012, Waterloo, Canada (P. Charpin);
- SAC 2012: August 16-17, 2012, Windsor, Ontario, Canada (A. Canteaut);
- *RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials*, September 2-7, 2012, St. Wolfgang Federal Institute, Austria (P. Charpin);
- YACC 2012, September 24-28, 2012, Porquerolles, France (A. Canteaut);
- Journées Codage et Cryptographie du GDR-IM, October 7-12, 2012, Dinard, France (A. Canteaut);
- Indocrypt 2012: December 9-12, 2012, Calcutta, India (N. Sendrier);
- FSE 2013: March 11-13, 2013, Singapore, Singapore (A. Canteaut, M. Naya-Plasencia);
- WCC 2013: April 15-19, 2013, Bergen, Norway (A. Canteaut, N. Sendrier);
- PQCrypto 2013: June 4-7, Limoges, France (N. Sendrier, JP Tillich);
- Asiacrypt 2013: December 1-5, Bengaluru, India (A. Canteaut, N. Sendrier);

8.1.3. Invited talks

- N. Sendrier. *Code-based Cryptography: Theory and Practice.* ARES, MoCrySEn 2012, Prague, Czech Republic, September 2012.
- N. Sendrier. *Code-based Cryptography.* Post-Quantum Cryptography and Quantum Algorithms, Lorentz Center, Leiden, The Netherlands, November 2012.
- D.E. Simos. *Families of Block Ciphers from Combinatorial Designs.* In Cryptography and its Applications in the Armed Forces (CAIAF2012) , Hellenic Military Academy "Evelpidon", Vari, Greece, April 2012.

8.1.4. Other responsibilities in the national community.

- N. Sendrier is a vice-chair of the "Commission d'Evaluation" at Inria;
- A. Canteaut is a member of the "Comité de pilotage" of the Fondation Sciences Mathématiques de Paris;
- JP Tillich is in charge of "Formation par la recherche" for the Paris-Rocquencourt center.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- A. Canteaut, *Stream ciphers*, 6 hours, M2, Telecom ParisTech, France;
- A. Canteaut, *Mathematical aspects of symmetric cryptography*, 3 hours, M2 (corps de Mines), Telecom ParisTech, France;
- A. Canteaut, *Advanced topics in symmetric cryptology*, 9 hours, M2, DTU, Denmark;
- J.-P. Tillich, *Algorithms and Programming*, 36 hours, M1, Ecole Polytechnique, France;
- J.-P. Tillich, *Introduction to Information Theory*, 32 hours, M2, Ecole Polytechnique, France.

8.2.2. Supervision

PhD: Christina Boura, *Sécurité et cryptanalyse des fonctions de hachage*, Université Pierre-et-Marie Curie, December 2012, supervisor: A. Canteaut

PhD: Stéphane Jacob, *Protection cryptographique des bases de données : conception et cryptanalyse*, Université Pierre-et-Marie Curie, March 2012, supervisor: A. Canteaut

PhD in progress: Mamdouh Abbara, *Quantum turbo-codes*, August 2009, supervisor: JP. Tillich.

PhD in progress: Marion Bellard, *Influence du mapping pour la reconnaissance d'un système de communication*, January 2011, supervisors: N. Sendrier and J.-P. Tillich

PhD in progress: Grégory Landais, *Mise en oeuvre des cryptosystèmes basés sur les codes correcteurs d'erreurs et de leurs cryptanalyse*, October 2010, supervisors: M. Finiasz and N. Sendrier

PhD in progress: Denise Maurice, *Quantum LDPC codes*, September 2010, supervisor : JP. Tillich.

PhD in progress: Rafael Misoczki, *Aspects of code-based cryptography*, November 2010, supervisor: N. Sendrier

PhD in progress: Jean-Christophe Sibel, *Decoding LDPC codes with many short cycles*, October 2009, supervisor : D. Declercq.

PhD in progress: Valentin Suder, *Les Permutations en Cryptographie Symétrique*, October 2011, supervisor: P. Charpin.

PhD in progress: Audrey Tixier, *Reconstruction of LDPC codes*, October 2012, supervisor: JP. Tillich

8.2.3. Juries

- Jean-Claude Carlach, *Contribution à la construction et au décodage à décision douce des codes correcteurs d'erreurs auto-duaux extrémaux*, Institut National des Sciences Appliquées de Rennes, February 2, 2012, committee: JP. Tillich.
- Stéphane Jacob, *Protection cryptographique des bases de données : conception et cryptanalyse*, Université Pierre-et-Marie Curie, March 8, 2012, committee: A. Canteaut (supervisor).
- Marine Minier, *Quelques résultats en cryptographie symétrique, pour les modèles de confiance dans les réseaux ambiants et la sécurité dans les réseaux de capteurs sans fil*, HDR, Université Lyon 1, May 31, 2012, committee: A. Canteaut.
- Pouyan Sepehrdad, *Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-Lightweight Symmetric Primitives*, Ecole Polytechnique Fédérale de Lausanne, Suisse, June 11, 2012, committee: A. Canteaut (reviewer).

- Matteo Gorgoglione, *Analyse et construction de codes LDPC non-binaires pour des canaux à évanouissement*, Université de Cergy-Pontoise, October 25, 2012, committee: JP. Tillich (reviewer).

- Anja Becker, *The representation technique – Applications to hard problems in cryptography*, UVSQ, Octobre 26, 2012, committee: N. Sendrier (reviewer).

- Matthieu Legeay, *Utilisation du groupe de permutations d'un code correcteur pour améliorer l'efficacité du décodage*, Université de Rennes 1, November 20, 2012, committee: N. Sendrier (reviewer).

- Christina Boura, *Sécurité et cryptanalyse des fonctions de hachage*, Université Pierre-et-Marie Curie, December 7, 2012, committee: A. Canteaut (supervisor).

- Sihem Mesnager, *Contributions aux fonctions booléennes pour la cryptographie symétrique et aux codes correcteurs d'erreurs*, HDR, Université Paris 8, December 10, 2012, committee: P. Charpin (reviewer), A. Canteaut.

- N. Delfosse, *Constructions et performances de codes LDPC quantiques*, Université Bordeaux I, December 12, 2012, committee: JP. Tillich (reviewer).

8.3. Popularization

- Anne Canteaut is a co-author of a paper on the state-of-the-art on the AES standard in the large-audience journal *MISC* [17].

- Lecture on cryptography at the *Journées Filles et Maths*, organized by Animath and Femmes et Sciences, for students in "Première" and "Terminale", IHP, Paris, December 21, 2012, A. Canteaut.

- Lectures (6h in total) to an audience of professors in "classes preparatoires" on quantum algorithms, Luminy, May 9, 2012, J.P. Tillich.

VEGAS Project-Team

7. Dissemination

7.1. Scientific Animation

Program and Paper Committee:

- Sylvain Lazard: Program committee of the ACM Symposium on Computational Geometry 2012 (SoCG'12) and of the European Workshop on Computational Geometry (EuroCG'12).
- Sylvain Petitjean: Program committee of the IEEE International Conference on Computer Vision and Pattern Recognition (CVPR'12).

Editorial responsibilities:

- Xavier Goaoc: Editor of the *Journal of Computational Geometry*.
- Sylvain Petitjean: Editor of *Graphical Models* (Elsevier).

Workshop organizations:

- Sylvain Lazard co-organized with S. Whitesides (Victoria University) the 11th Inria - McGill - Victoria Workshop on Computational Geometry [2] (Bellairs Research Institute of McGill University) in Feb. (1 week workshop on invitation).
- Xavier Goaoc was co-organiser of the *Journées de Géométrie Algorithmique* 2012 (http://jga2012. fr). This event gathered the french community of computational geometry (50-60 participants) for one week.
- Xavier Goaoc was co-organiser of *Algorithms & Permutations* 2012 (http://igm.univ-mlv.fr/AlgoB/ algoperm2012/). This event gathered $\sim$ 70 participants from theoretical computer science for two days.
- Xavier Goaoc organized a *workshop on interactions between stochastic and computational geometries* (http://webloria.loria.fr/~goaoc/ANR-Presage/meetings.html) where 21 participants, on invitation, worked for a week on research problems at the interface between stochastic and computational geometries.

Other responsibilities:

- Sylvain Lazard: Head of the Inria Nancy-Grand Est *PhD and Post-doc hiring committee* (since 2009). Member of the *Bureau du Département Informatique de Formation Doctorale* of the *École Doctorale IAE+M* (since 2009). Member of the hiring committee for St Dié assistant professor position. Chargé de formation par la recherche for Inria Nancy-Grand Est.
- Laurent Dupont: *Responsible* of admissions of IUT Charlemagne, University Nancy 2 (September 2011- September 2012). *Member* of Commission Pédagogique Nationale Infocom/SRC (since 2011). *Member* of Commission Information Scientifique (Inria/Loria).
- Xavier Goaoc: Chair of the Inria *COST-GTRI committee* (since 2011).
- Guillaume Moroz: Member of the organizing committee of the *Olympiades académiques de mathématiques*. *Vice delegate* of the *Commission des Utilisateurs des Moyens Informatiques pour la Recherche*. Invited to give a course at Young researcher School EJCIM 2012 and doctoral school of science and technology of Versailles.
- Sylvain Petitjean: Until August: *Scientific delegate* of Inria Nancy Grand-Est and chairman of its *Project committee* (since 2009). Member of the *Executive committee* of Inria Nancy Grand-Est, member of its *Commission des développements technologiques*. Member of Inria's *Evaluation committee*. Since September: Acting director of the Inria Nancy Grand-Est. Member of Inria's *Executive committee*.
- Marc Pouget: Member of the CGAL Editorial Board (since 2008).

---

[2] Workshop on Computational Geometry

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Master: Marc Pouget and Xavier Goaoc, *Introduction à la géométrie algorithmique*, 10.5 HETD, M1, École Nationale Supérieure de Géologie, France

Master: Xavier Goaoc, *Recherche opérationnelle*, 25 HETD, M1, École des Mines de Nancy.

Master: Xavier Goaoc, *Pépites en géométrie algorithmique*, 4.5 HETD, M1, École des Mines de Nancy.

Licence: Laurent Dupont, *Systèmes de Gestion de Bases de Données Avancé*, 40h, Université de Lorraine (IUT Charlemagne).

Licence:Laurent Dupont, *Concepts et Outils Internet*, 40h, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Programmation Objet et Évènementielle*, 40h, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont, *Rich Internet Applications*, 40h, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont and Yacine Bouzidi, *Programmation de Sites Web Dynamiques*, 68h, Université de Lorraine (IUT Charlemagne).

Licence: Laurent Dupont and Yacine Bouzidi, *Algorithmique*, 76h, Université de Lorraine (IUT Charlemagne).

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

7.2.2. Supervision

PhD in progress : Yacine Bouzidi, Résolution de systèmes algébriques bivariés et topologie de courbes planes, started in October 2010, Sylvain Lazard et Marc Pouget

PhD in progress : Fabien Mathieu, Simulation numériques 3D pour le prototypage rapide par Stratoconception, thèse CIFRE with CIRTES, started in February 2012 and stopped in September 2012 for administrative reasons, Sylvain Lazard.

7.2.3. Juries

- Xavier Goaoc was on the reading and defense committees of the thesis of Daniela Maftuleac, Aix-Marseille Univ, Juin 2012.

ALF Project-Team

9. Dissemination

9.1. Scientific community animation

- Pierre Michaud was a member of the ISPASS 2012 and MuCoCos 2012 program committees
- Isabelle Puaut is a member of the program committees of ECRTS 2013, RTAS 2013 and RTCSA 2013. She was a member of the program committee of DAC 2012, ECRTS 2012, EFTA 2012, LCTES 2012, RTCSA 2012, RTNS 2012, WCET 2012.
- André Seznec was a member of Micro 2012, ISCA 2012 and ICDD2012 program committees. He is a member of the editorial board of the IEEE Micro.
- André Seznec is the Program co-chair of HiPEAC 2013, January 2013 and Program co-chair of PACT 2013 (September 2013).
- Erven Rohou was a member of the program committees of PARMA 2012, EUC 2012 and Computing Frontiers 2012.

9.2. Teaching

- F. Bodin, A. Seznec, I. Puaut and E. Rohou are teaching computer architecture and compilation in the master of research in computer science at University of Rennes I.
- Erven Rohou teaches classes and labs of Computing Systems at école Polytechnique (INF422).
- I. Puaut teaches operating systems and real-time systems in the master degree of computer science of the University of Rennes I and at Ecole Supérieure d'ingénieurs de Rennes.
- D. Hardy teaches operating systems and compilers in the master degree of computer science of the University of Rennes I. He teaches real-time systems in the BSc degree *Embedded automotive systems*.
- Pierre Michaud and André Seznec are teaching computer architecture at the engineering degree in computer science at Ecole Supérieure d'ingénieurs de Rennes.
- I. Puaut is co-responsible of the Master of Research in computer science in Britanny (administered jointly by University of Rennes I, University of Bretagne Sud, University of Bretagne Occidentale, INSA de Rennes, ENS Cachan antenne de Bretagne, ENIB, Supélec, Telecom-Bretagne).

9.3. Workshops, seminars, invitations, visitors

9.3.1. Seminars

- A. Seznec has presented a seminar on "What you will never have wanted to know on branch prediction" at University of Cyprus (April 2012), ETH Zurich (May 2012), Qualcomm (August 2012, Raleigh, North Carolina), Georgia Tech (August 2012) and ARM Sophia Antipolis (October 2012).
- A. Seznec has presented invited talks on "Should we defy the Amdahl's Law" at MATEO 2012 workshop in honor of Mateo Valero (Barcelona, June 2012), and at the "Let's Imagine the Future Workshop" in honor of Jean-Pierre Banâtre (Rennes, November 2012).
- A. Seznec has presented a seminar on "Revisiting value prediction" at Intel Hillsboro in December 2012.
- A. Seznec has presented a seminar on "HAVEGE, HArdware Volatile Entropy Gathering and Expansion: unpredictable random number generation at user level" at the LPMA laboratory (Paris, September 2012).

- I. Puaut has presented a seminar on "WCET estimation for multi-core architectures" at CNES, Toulouse, in December 2012.

- Pierre Michaud has presented a seminar on "Hardware acceleration of sequential loops" at Intel, Boston in December 2011.

- E. Rohou gave a talk at the GDR GPL/5es journées françaises de compilation: "Défis des architectures à venir - Quelle compilation pour demain ?" (Rennes, Irisa/Inria April 2012)

- E. Rohou gave an invited talk at Harvard University: "Compilation Challenges for Upcoming Architectures", (September 2012)

- E. Rohou gave a invited talk at the Workshop on Language Virtual Machines and Multicore Architectures: "Compilation Challenges for Future Architectures" (September 2012, LIP6 Paris)

- E. Rohou gave an invited talk at the Egypt-Japan University of Science and Technology in Alexandria:"Performance of Future Architectures and Compilation Challenges" (May 2012).

9.3.2. *Visits*

- Pr Ahmed El-Mahdy, from the Egyptian-Japanese University of Science and Technology visited the ALF project for 1 week in October 2012.

- Pr Qureshi from Georgia Tech visited the ALF project-team for 3 weeks in July 2012 in the framework of the DAL ERC project.

- Pr Baniasidi from Victoria university visited the ALF project-team for 1 week in October 2012. This visit was funded by the French embassy in Canada.

- Keisuke Kuroyanagi from University of Tokyo was a master intern in the ALF team from April 2012 to July 2012. He worked on memory scheduling [21].

9.4. Miscelleanous

- I. Puaut is a member of the advisory board of the foundation Michel Métivier (http://www.fondation-metivier.org).

- I. Puaut is a member of the Technical Committee on Real-Time Systems of Euromicro, which is responsible for ECRTS, the prime European conference on real-time systems.

- I. Puaut is in the steering committee of the RTNS conference.

- I. Puaut is the french representative for the COST action TACLe (Timing Analysis on Code-Level), for which she also chairs the student mobility committee.

- Erven Rohou was a member of the working group GTInria2020 whose mission is to produce the next "Plan Stratégique".

- A. Seznec is an elected member of the scientific committee of Inria.

- A. Seznec has been nominated by ACM for 3 years 2011-2013 on the selection committee for the ACM-IEEE Eckert-Mauchly award.

- A. Seznec was a member of the steering committee of ISCA 2012.

- E. Rohou has been appointed "correspondant scientifique des relations internationales" for Inria Rennes Bretagne Atlantique.

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

8. Dissemination

8.1. Scientific Animation

D. Chillet was General Co-Chair of the Conference on Design and Architectures for Signal and Image Processing (DASIP) in Karlsruhe, Germany, Oct. 2012.

D. Chillet was the Editor of a Special Issue of International Journal of Real Time Image Processing, 2012.

A. Tisserand was a member of technical program committee of the following conferences: IEEE ARITH'21, IEEE Reconfig 2012, DASIP 2012, IEEE NEWCAS 2012. He is a member of the editorial board of the International Journal of High Performance Systems Architecture, Inderscience.

M. Gautier was a member of the technical program committee of IEEE VTC-fall 2012, IEEE ICCVE 2012 and IARIA COCORA 2012.

E. Casseau co-organized with Michael Hubner the first DASIP demo night during the Conference on Design and Architectures for Signal and Image Processing, Karlsruhe, Germany. Details on http://ecsi.org/dasip2012/demo-night.

S. Pillement and E. Casseau were members of the Program Committee of DASIP.

P. Quinton was the coordinator of the "équipe projet de recherche" PucesCom of the Université européenne de Bretagne.

O. Sentieys was a member of technical program committee of the following conferences: IEEE/ACM DATE, IEEE ISQED, IEEE VTC, IEEE DDECS, DCIS, FTFC. He was Track Chair at NEWCAS. He is on the editorial board of Journal of Low Power Electronics, American Scientific Publishers, and of ISRN Sensor Networks.

O. Sentieys is a member of the steering committee of the GDR SOC-SIP. He is the chair of the IEEE Circuits and Systems (CAS) French Chapter. In 2011, he was an expert for some scientific organizations (ANR INS, ANR blanc). He is a member of Allistene working group.

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

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

A. Tisserand co-organized the ECOFAC 2012 *école thématique CNRS conception faible consommation pour les systèmes embarqués temps réel* in La Colle-sur-Loup, May 21–25, 2012. Details on http://leat.unice.fr/ECoFaC2012/.

8.2. Seminars and Invitations

A. Tisserand gave an invited talk at the French *Rencontres Arithmétique de l'Informatique Mathématique du GT ARITH - GDR IM* in June on *Circuits for True Random Number Generation with On-Line Quality Monitoring*.

A. Tisserand gave a invited lecture at the CNRS ECOFAC 2012 spring school on *Power Consumption and Security: Attacks and Countermeasures*.

A. Tisserand gave a invited lecture at the IRMAR (Maths) Laboratory of University of Rennes 1 on *True Random Number Generation with On-Line Quality Monitoring*.

8.3. Teaching - Supervision - PhD Committee

8.3.1. Teaching Responsibilities

There is a strong teaching activity in the CAIRN team since most of the permanent members are Professors or Associate Professors.

C. Wolinski is the Director of ESIR.
P. Quinton is the deputy-director of Ecole Normale Supérieure de Cachan, responsible of the Brittany branch of this school.
D. Chillet is the Director of Academic Studies of ENSSAT.
P. Scalart is the Head of the Electronics Engineering department of ENSSAT.
S. Derrien is the responsible of the first year of the master of computer science at ISTIC since Sep. 2012.
O. Sentieys is responsible of the "Embedded Systems" branch of the SISEA Master of Research (M2R).

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.
M2R stands for Master by Research, second year.

D. Chillet is member of the French National University Council since 2009 in signal processing and electronics (Conseil National des Universités en 61e section).
D. Chillet is member of the Permanent Committee of the French National University Council since november 2011 in signal processing and electronics (Commission Permanente du Conseil National des Universités en 61e section).

8.3.2. Teaching

O. Berder: introduction to signal processing, 38h, ENSSAT(L3)

O. Berder: microprocessors and digital systems, 19h, ENSSAT(L3)

O. Berder: wireless communications, 23h, ENSSAT(M2)

O. Berder: digital signal processing, 60h, ENSSAT(M1)

O. Berder: ad hoc networks, 58h, ENSSAT(M1-M2)

O. Berder: signal processing, 24h, IUT Lannion (L2)

E. Casseau: verification, 12h, Master by Research and ENSSAT(M2)

E. Casseau: hardware description language, 20h, ENSSAT(M1)

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

E. Casseau: real time design methodology, 24h, ENSSAT(M1)

E. Casseau: verification, 25h, USTH (M1)

E. Casseau: signal processing, 16h, ENSSAT(L3)

S. Derrien: component and system synthesis, 16h, Research Master (MRI ISTIC) (M2)

S. Derrien: computer architecture, 12h, ENS Cachan (L3)

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

F. Charot: specification of applications with the signal synchronous language, 24h, ESIR(M1)

F. Charot: virtual prototyping of multiprocessor system-on-chip, 24h, ESIR(M1)

F. Charot: design of embedded systems, 28h, ESIR(M1)

D.Chillet: Basic processor architecture, 20h, ENSSAT(L1)

D.Chillet: Design methodology of real-time systems, 32h, Enssat(L2)

D.Chillet: Advanced processor architectures, 24h, Enssat(M2)

D.Chillet: Multimedia processor architectures, 24h, Enssat(M2)

D.Chillet: Multi-processor systems, 20h, Enssat(M2)

D. Chillet: advanced processors architectures, 24h, Master by Research and Enssat(M2)

D. Chillet: low-power digital CMOS circuits, 6h, Telecom Bretagne and University of Occidental Brittany (UBO) (M2)

D. Chillet: Digital system design, 25h, University of Science and Technology of Hanoi, (M1)

D. Chillet: Advanced Multiprocessor system , 25h, University of Science and Technology of Hanoi, (M2)

M.Gautier, electronics, 42h, IUT Lannion (L1)

M.Gautier, telecommunications, 114h, IUT Lannion (L1)

R. Rocher: electricity, 16h, IUT Lannion (L1)

R. Rocher: electronics, 44h, IUT Lannion (L1)

R. Rocher: telecommunications, 82h, IUT Lannion (L1)

R. Rocher: signal processing, 12h, IUT Lannion (L2)

R. Rocher: digital communications, 48h, IUT Lannion (L2)

P. Scalart: non-linear optimisation, 18h, Master by Research and ENSSAT (M2)

P. Scalart: Parametric modelisation, optimal and adaptive Filters, 24h, Master by Research and ENSSAT (M2)

P. Scalart: source coding, 14h, Master by Research and ENSSAT (M2)

P. Scalart: cellular networks, 24h, ENSSAT (M2)

P. Scalart: digital communication systems, 32h, ENSSAT (M1)

P. Scalart: random signals and systems, 12h, ENSSAT (M1)

O. Sentieys: methodologies for system-on-chip design, 6h, Master by Research and Enssat(M2)

O. Sentieys: VLSI integrated circuit design, 66h, Enssat(M1)

O. Sentieys: high-level synthesis of digital signal processors, 16h, Master by Research and Enssat(M2)

A. Tisserand: GPU programming, 8h, Enssat(M2)

A. Tisserand: hardware computer arithmetic operators, 6h, Master by Research, Univ. Rennes 1 (M2)

A. Tisserand: computer arithmetic, 12h, ENS Cachan, Antenne de Bretagne, *Magister* Computer Science and Telecommunications (L3)

A. Tisserand: computer arithmetic, 16h, ENSEIRB, (L3)

C. Wolinski: architecture 1, 64h, Esir(L3)

C. Wolinski: architecture 2, 28h, Esir(L3)

C. Wolinski: design of embedded systems, 48h, Esir(M1)

C. Wolinski: signal, image, architecture, 26h, Esir(M1)

C. Wolinski: programmable architectures, 10h, Esir(M1)

C. Wolinski: component and system synthesis, 10h, Master by Research (MRI ISTIC) (M2)

8.3.3. Supervision

HDR: Olivier Berder, Systèmes multi-antennes et optimisation énergétique des réseaux de capteurs sans fil, Habilitation à Diriger des Recherches, University of Rennes 1, Dec. 2012.

PhD: Naeem Abbas, Acceleration of a Bioinformatics Application using High-Level Synthesis, May 2012, P. Quinton, S. Derrien.

PhD: Andrei Banciu, A Stochastic Approach for the Range Evaluation, Feb. 2012, E. Casseau.

PhD: Antoine Eiche, Real-Time Scheduling for Heterogeneous and Reconfigurable Architectures using Neural Network Structures, University of Rennes 1, Sep. 2012, D.Chillet.

PhD: Antoine Floc'h, Optimizing Compilation for Processor Instruction-Set Extension, Jun. 2012, C. Wolinski, F. Charot.

PhD: Quoc-Tuong Ngo, Generalized minimum Euclidean distance based precoders for MIMO spatial multiplexing systems, Jan. 2012, P. Scalart, O. Berder.

PhD: Danuta Pamula, Arithmetic operators on $GF(2^m)$ for cryptographic applications: performance - power consumption - security tradeoffs, University of Rennes 1 and Silesian University of Technology, Dec. 2012, A. Tisserand.

PhD: Le-Quang-Vinh Tran, Energy-efficient cooperative relay protocols for wireless sensor networks, Dec. 2012, O. Berder, O. Sentieys.

PhD: Karthick Parashar, System-level approaches for fixed-point refinement of signal processing algorithms, Dec. 2012, O. Sentieys, D. Menard.

PhD: Chenglong Xiao, Custom Operator Identification for High-level Synthesis, University of Rennes 1, Nov. 2012, E. Casseau.

PhD in progress: Mahtab Alam, Power Aware Signal Processing for Reconfigurable Radios in the context of Wireless Sensor Networks, Nov. 2009, O. Sentieys, O. Berder, D. Menard.

PhD in progress: Djamel Benfarhat, Design of disruption-tolerant communication protocols for mobile communicating objects in health applications, 2009, Patrice Quinton jointly with Frédéric Guidec, IRISA UBS.

PhD in progress: Karim Bigou, RNS Hardware Units for ECC, Oct. 2011, A. Tisserand.

PhD in progress: Robin Bonamy, Power Consumption Modelling and Optimisation for Reconfigurable Platform, Oct. 2009, D. Chillet.

PhD in progress: Franck Bucheron, Secure Virtualization for Embedded Systems, Oct. 2011, A. Tisserand.

PhD in progress: Thomas Chabrier, Reconfigurable Arithmetic Units for Cryptoprocessors with Protection against Side Channel Attacks, Oct. 2009, A. Tisserand, E. Casseau.

PhD in progress: Aymen Chakhari, Analytical approach for decision errors in fixed-point digital communication systems, Oct. 2010, R. Rocher, P. Scalart.

PhD in progress: Ali-Hassan El-Moussaw, Performance/Accuracy Trade-Off in Automatic Parallelization for Embedded Many-Core Platforms, Nov. 2012, S. Derrien.

PhD in progress: Clément Guy, Generic Definition of Domain Specific Analysis using MDE, Oct. 2010, S. Derrien, jointly with J.M. Jezequel and B. Combemale from Triskell EPI.

PhD in progress: Christophe Huriaux, Embedded reconfigurable hardware accelerators with efficient dynamic reconfiguration management, Oct. 2012, O. Sentieys, A. Courtay.

PhD in progress: Quang-Hai Khuat, Real-Time Spatio-Temporal Task Scheduling on 3D Architectures, Oct. 2011, D. Chillet.

PhD in progress: Trong-Nhan Le, Global power management system for self-powered autonomous wireless sensor nodes, Jan. 2011, O. Sentieys, O. Berder.

PhD in progress: Quang-Hoa Le, Virtualized dynamic reconfiguration for 3D SoC, Oct. 2012, E. Casseau, A. Courtay.

PhD in progress: Jérémie Métairie, Reconfigurable Arithmetic Units for Secure Cryptoprocessors, Oct. 2012, A. Tisserand, E. Casseau.

PhD in progress: Antoine Morvan, Loop Transformations for Design Space Exploration in High-Level Synthesis, Oct. 2009, P. Quinton, S. Derrien.

PhD in progress: Jean-Charles Naud, Source-to-Source Code Transformation for Fixed-Point Conversion, Oct. 2009, D. Menard, O. Sentieys.

PhD in progress: Viet-Hoa Nguyen, Energy-efficient cooperative techniques for Wireless Body Area Sensor Networks, Nov. 2012, O. Berder, jointly with C. Langlais from Telecom Bretagne.

PhD in progress: Matthieu Texier, Low-Power Embedded Multi-Core Architectures for Mobile Systems, Oct. 2009, O. Sentieys, jointly with R. David from CEA List.

PhD in progress: Michel Theriault, Transmit Beam-forming for Distributed Wireless Access with Centralized Signal Processing, Oct. 2007, O. Sentieys, jointly with S. Roy from U. Laval, Canada.

PhD in progress: Vivek D. Tovinakere, Ultra-Low Power Reconfigurable Controllers for Wireless Sensor Networks, Oct. 2009, O. Sentieys.

Ganda-Stéphane Ouedraogo, Automatic synthesis of hardware accalerator from high-level specifications in flexible radios, Oct. 2011, M. Gautier, O. Sentieys.

PhD in progress: Pramod P. Udupa, Sampling, synchronising, digital processing and FPGA implementation of 100Gbps optical OFDM signals, Jan. 2011, O. Sentieys.

PhD in progress: Hervé Yviquel, Video coding design framework based on SoC-based platforms, Oct. 2010, E. Casseau.

PhD in progress: Zhongwei Zheng, Short-range geolocation algorithms based on distributed multi-sensor processing, Nov. 2012, P. Scalart, jointly with C. Roland from Lab-STICC.

8.4. Popularization

A. Tisserand gave a popularization talk at *Fête de la science* 2012 in Lannion on *low-energy electronic circuits*.

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

8. Dissemination

8.1. Scientific Animation

Vincent Loechner co-organized IMPACT 2012, the 2nd International Workshop on Polyhedral Compilation Techniques, in conjunction with the HiPEAC conference in January 2012. Out of 13 received submissions, 6 were accepted as regular papers and 4 as tool demonstrations, and presented along a keynote by Keshav Pingali.

Philippe Clauss and Vincent Loechner are part of the program committee of IMPACT 2013.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Vincent Loechner, programmation système et réseau, 30, L2, University of Strasbourg, France

Licence : Vincent Loechner, fondements des systèmes d'exploitation, 33, L3, University of Strasbourg, France

Master : Vincent Loechner, système et programmation temps-réel, 25, M1, University of Strasbourg, France

Master : Vincent Loechner, compilation avancée, 6, M1, University of Strasbourg, France

Master : Vincent Loechner, parallélisme, 28, M2, University of Strasbourg, France

Master : Vincent Loechner, calcul parallèle, 30, école d'ingénieur (5ième année), University of Strasbourg, France

Master : Vincent Loechner, langage interprété, 40, M1, University of Strasbourg, France

Master : Vincent Loechner, TP programmation, 10, M1, University of Strasbourg, France

Licence : Julien Narboux, Culture et Pratique de l'Informatique, 18, L1, University of Strasbourg, France

Licence : Julien Narboux, Logique et Programmation Logique, 61 , L2, University of Strasbourg, France

ENSIIE : Julien Narboux, Logique, 31 , 1a, ENSIIE, France

Master: Julien Narboux, Ingénierie de la preuve, 27 , M1, University of Strasbourg, France

Master: Julien Narboux, Certification du Logiciel, 36 , M2, University of Strasbourg, France

Master: Julien Narboux, Suivi apprentissage, 50, M1-M2, University of Strasbourg, France

Master: Julien Narboux, Encadrement TER, -, M1, University of Strasbourg, France

Master: Julien Narboux, Encadrement Projet Individuel (1 étudiant), -, M2, University of Strasbourg, France

Master: Julien Narboux, Encadrement Projets de Groupe 140h (25 étudiants), 10, M2, University of Strasbourg, France

Master: Julien Narboux, Soutenances d'apprentissage, 10, M2, University of Strasbourg, France

Licence : Nicolas Magaud, Méthodologie du Travail Universitaire, 12, L1, University of Strasbourg, France

Licence : Nicolas Magaud, Projet professionnel personnel, 20, L1, University of Strasbourg

Licence : Nicolas Magaud, Structures de données et Algorithmes 2, 22, L2 Informatique, University of Strasbourg

Licence : Nicolas Magaud, Informatique : Algorithmique et Structures de Données, 20, L3 Mathématiques, University of Strasbourg

Licence : Nicolas Magaud, Pratique des systèmes d'exploitation (PSE), 16, L2 Informatique, University of Strasbourg

Master: Nicolas Magaud, Ingénierie de la preuve, 18 , M1, University of Strasbourg, France

Master: Nicolas Magaud, Suivi apprentissage, 60, M1-M2, University of Strasbourg, France

ENSIIE : Nicolas Magaud, Introduction à la Programmation Fonctionnelle, 52 , 1a, ENSIIE, France

CNAM Alsace : Nicolas Magaud, Algorithmique, 40, 1a, CNAM Alsace, France

Licence : Éric Violard, Programmation système & réseau, 60 , L2, University of Strasbourg, France

Licence : Éric Violard, Programmation fonctionnelle, 42 , L2, University of Strasbourg, France

Licence : Éric Violard, Bases de données, 8 , L2, University of Strasbourg, France

Master : Éric Violard, Compilation, 54, M1, University of Strasbourg, France

Master : Éric Violard, Sémantique, 45, M1, University of Strasbourg, France

Master : Alain Ketterlin, Compilation, 64 , M1, University of Strasbourg

Master : Alain Ketterlin, Compilation avancée, 20 , M1, University of Strasbourg

Master : Alain Ketterlin, Suivi d'apprenti, 12 , M1, University of Strasbourg

Master : Philippe Clauss, Compilation avancée, 30 , M1, University of Strasbourg

Master : Philippe Clauss, Système et Programmation Temps-réel, 30 , M1, University of Strasbourg

Master : Philippe Clauss, OS embarqués, 30 , M1, University of Strasbourg

8.2.2. Supervision

PhD : Alexandra Jimborean, Adapting the polytope model for dynamic and speculative parallelization, University of Strasbourg, September the 14th 2012, Philippe Clauss and Vincent Loechner

PhD in progress : Aravind Sukumaran-Rajam, Enlarging the scope of polyhedral speculative parallelization, November 2012, Philippe Clauss and Alain Ketterlin

PhD in progress : Jean-François Dollinger, Heterogeneous speculative parallelization, September 2010, Vincent Loechner and Philippe Clauss

PhD in progress : Imèn Fassi, Multifor for Multicore, September 2012, Philippe Clauss and Yosr Slama

8.2.3. Juries

Philippe Clauss participated to the following HDR jurys in 2012:

Date	Candidate	Place	Role
Dec. 7	Fabrice Rastello	École Normale Supérieure de Lyon	Reviewer
Déc. 12	Cédric Bastoul	Univ. Paris-Sud	Examiner

Philippe Clauss participated to the following PhD jurys in 2012:

Date	Candidate	Place	Role
July 3	Oussama Gamoudi	Univ. Pierre et Marie Curie, Paris	Reviewer
Oct. 2	Artur Pietrek	Univ. Grenoble	Reviewer
Oct. 22	Andrés Salim Charif-Rubial	Univ. Versailles	Reviewer
Dec. 13	Mehdi Amini	École des Mines, Paris	Examiner

COMPSYS Project-Team

9. Dissemination

9.1. Scientific Animation

Christophe Alias is a member of the steering committee of IMPACT (international workshop on polyhedral compilation techniques). Christophe Alias, Alain Darte, and Paul Feautrier were members of the program committee of IMPACT'13, which will be held in conjunction with HiPEAC'13.

Laure Gonnord and Fabrice Rastello are the co-animators of the french compilation community, and organized the fifth session in June 2012, in Rennes.

Paul Feautrier is an associate editor of *International Journal of Parallel Programming* and of *Prallel Computing*. Alain Darte is an associate editor of ACM Transactions on Embedded Computing Systems.

Laure Gonnord was a member of the program commitee of TAPAS'12 (Tools for Automatic Program Analysis).

In addition to IMPACT'13, Paul Feautrier is a member of the program committee of ParCo'13 (International Parallel Computing Conference). He has reviewed papers for LCTES, DATE and ACM TECS.

In addition to IMPACT'13, Alain Darte was a member of the program committees of DATE'13 (Design, Automation, and Test in Europe), LCTES'12 (Languages, Compilers, Tools, and Theory for Embedded Systems), IPDPS'13 (International Parallel and Distributed Processing Symposium). He has reviewed papers for the DATE'13, LCTES'12, EMSOFT'12, CGO'13 conferences and for the following journals: TSI, Parallel Computing, ACM TECS.

9.2. Workshops and Invited Talks

Alain Darte and Quentin Colombet participated to the 3-days workshop CPC'12 (16th Workshop on Compilers for Parallel Computing), in Padova, Italy, January 11-13, 2012. giving two talks "Kernel offloading with optimized remote accesses" and "Spilling in the light of SSA".

Alain Darte was invited by Jürgen Teich (University of Erlangen-Nuremberg) to give a talk (May 18, 2012) on "Optimizing remote accesses for offloaded kernels, with application to HLS for FPGA", as part of their "invasive computing" project.

Alain Darte was invited to participate to the 4-days workshop ScalPerf'12 (Scalable Approaches to High Performance and High Productivity Computing), in Bertinoro, Italy, September 23-27, 2012. He gave a talk on "Parametric tiling with pipelining or how to automate double-buffering execution style".

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Licence: Christophe Alias gave a L3 course on "Introduction to compilation" at ENSI Bourges and a L2 lab on "Architecture des ordinateurs" at Université Lyon 1. Laure Gonnord has a full teaching activity in Polytech'Lille where she teaches algorithmics, compilation, and basics of hardware.

Master 1: Christophe Alias gave a Master 1 course on "Compilation" at ENS-Lyon.

Master 2: Alain Darte gave a full Master 2 course on "Advanced compilation and program optimizations" at ENS-Lyon.

Master 1 and 2: Christophe Alias is organizer of the Winter Master School "Vérification et certification du logiciel" that was held in January 2012 at ENS-Lyon, as part of the Master of ENS-Lyon.

Internships: Laure Gonnord and Christophe Alias co-supervised the undergraduate internship of Jean-Marie Vincenti, from the Engineering School Polytech'Lille. This internship lasted two months, from June 2012 to July 2012. The topic was about graphical visualization and step-by-step debugging of communicating processes described with an execution trace. Alain Darte advised the M2 internship of Alexandre Isoard on the parametric tiled kernel offloading (see Section 6.5).

9.3.2. Supervision

PhD in progress: Guillaume Iooss, "Semantic program transformations in the polyhedral model", started in September 2011, at ENS-Lyon and Colorado State University. Advisors: Christophe Alias, Alain Darte, Sanjay Rajopadhye (Colorado State University).

PhD in progress: Alexandre Isoard, "Optimization of remote communications", started in September 2012, at ENS-Lyon. Advisors: Christophe Alias, Alain Darte.

PhD: Quentin Colombet, "Decoupled (SSA-based) Register Allocators: from Theory to Practice, Coping with Just-In-Time Compilation and Embedded Processors Constraints" [1], ENS-Lyon, December 7, 2012. Advisors: Alain Darte, Fabrice Rastello.

HdR: Fabrice Rastello, "On Sparse Intermediate Representations: Some Structural Properties and Applications to Just In Time Compilation" [2], ENS-Lyon, December 7, 2012.

9.3.3. Juries

Fabrice Rastello was member of the jury for Artur Pietrek's PhD thesis (Verimag, Université Joseph Fourier), defended December 2, 2012.

Paul Feautrier is one of the referees for Stephane Mancini's HdR (TIMA, Grenoble), to be defended February 19, 2013.

Alain Darte was reviewer of Mehdi Amini's PhD thesis (Ecole nationale supérieure des Mines de Paris), defended December 13, 2012, and entitled "Source-to-Source Automatic Program Transformations for GPU-like Hardware Accelerators".

As co-advisors, Alain Darte and Fabrice Rastello were of course part of the jury of Quentin Colombet's PhD thesis [1], defended December 7, 2012, at ENS-Lyon, and entitled "Decoupled (SSA-based) Register Allocators: From Theory to Practice, Coping with Just-In-Time Compilation and Embedded Processors Constraints".

Alain Darte was part of the jury of Fabrice Rastello's HdR thesis [2], defended December 7, 2012, at ENS-Lyon, and entitled "On Sparse Intermediate Representations: Some Structural Properties and Applications to Just-In-Time Compilation".

AOSTE Project-Team

9. Dissemination

9.1. Scientific Animation

Robert de Simone

Technical Program Committee: FDL2012, SIES2012, SSMBSE2012, MEMOCODE2012, ES-Lsyn2012.

Board of Administrators: CIM PACA Design Platform association

Scientific co-animator: DAS SE (Specific Action Domain on Embedded Systems), Aerospace Valley Competitiveness Cluster

Yves Sorel

Technical Program Committee: RTNS 2012, DASIP 2012.

Editorial Board: Traitement du Signal Journal

Steering Committee: OCDS/SYSTEM@TIC Paris-Region Cluster

Frédéric Mallet

Technical Program Committee: ESLsyn2012.

Laurent George

Technical Program Committee: ECRTS 2012, RTAS 2012, WFCS 2012.

Co-editor: special issue of Real-Time Systems Journal made of best papers from RTNS 2011 conference (with Alan Burns, Univ. of York, UK).

Scientific Co-chair: ACTRISS group, supported by GDR ASR (CNRS, France) (http://www.actriss.org/).

Julien Deantoni

Technical Program Committee: CIEL2012.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: Julien Deantoni, Computer Environnement, 30 h, L2 level, Polytech engineering school of University Nice/Sophia-Antipolis (UNS EPU) France.

Master:Julien Deantoni, Model Driven Engineering, 22 h, M2, UNS EPU.

Master : Julien Deantoni, C++ and Object Oriented Programming, 54 h, M1, UNS EPU.

Master: Julien Deantoni, Embedded Software and systems, 7 h, M2, UNS EPU.

Master: Julien Deantoni, VHDL, 40 h, M1, UNS EPU.

Licence: Sid-Ahmed-Ali Touati, Assembleurs et jeux d'instructions, 52h, L3, UNS Licence info.

Licence: Sid-Ahmed-Ali Touati, Systèmes informatiques, 30h, L1, UNS Licence info.

Master: Sid-Ahmed-Ali Touati, Programmation efficaces pour programmes embarqués et hautes performances, 16h, M1 Master ISI.

Master: Sid-Ahmed-Ali Touati, Systèmes d'exploitation avancés, 39h, M1, UNS Master ISI.

Master: Sid-Ahmed-Ali Touati, Programmation efficace et Optimisation de code, 16h, M1, UNS Master ISI.

Master: Sid-Ahmed-Ali Touati, Architecture des Processeurs, 15h, M1, UNS EPU.

Licence : Frédéric Mallet, Introduction à la Programmation Objet, 45h, L1, UNS.

Licence: Frédéric Mallet, Architecture des ordinateurs, 45h, L3, UNS.

Master: Frédéric Mallet, Programmation Avancée et Design Patterns, 93h, M1, UNS.

Master: Frédéric Mallet, Java pour l'Informatique Industrielle, 24h, M1, UNS.

Master: Frédéric Mallet, Architectures des ordinateurs, 12h, M1, UNS.

Master: Frédéric Mallet, Formal Models for Network-On-Chips, 3h, M2, UNS.

Licence : Marie-Agnes Peraldi-Frati, Algorithms and programming 60h,L1, UNS Institute of technology.

Licence : Marie-Agnes Peraldi-Frati, System and Networks administration 80h, L2, UNS Institute of technology .

Licence :Marie-Agnes Peraldi-Frati, Web Programming 50 h , L2, UNS Institute of technology.

Master : Robert de Simone, Formal Models for Networks-on-Chip, 24h , M2, UNS.

Master : Robert de Simone, Semantics of Embedded and Distributed Systems, 24 h, M1, UNS.

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

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

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

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

Master: Dumitru Potop, Programmation synchrone des systèmes temps-réel, 8h, M1, EPITA Engineering School Paris

Licence: Laurent George, Java and Shell programming 48h, L1, IUT RT UPEC

Master: Laurent George, Distributed Real-Time Systems, 24h, M2, UPEC

9.2.2. Supervision

PhD: Mohamed Marouf, *Ordonnancement temps réel dur multiprocesseur tolérant aux fautes appliqué à la robotique mobile*, Ecole des Mines de Paris, defended on June 1st 2012, supervised by Yves Sorel, co-supervised by Brigitte D'Andrea-Novel (Institut Mines-Telecom).

PhD in progress: Carlos Ernesto Gomez-Cardenas,*Environnement multi-vues pour la métamodélisation sémantique formelle de systèmes embarqués*, UNS, started September 2010, supervised by Frédéric Mallet.

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

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

PhD in progress: Ying Lin, *Formal Analysis of polychronous models with MARTE/CCSL*, East China Normal University, started September 2011, supervised by Jing Liu (ECNU), co-supervised by Frédéric Mallet.

PhD in progress: Falou Ndoye, *Multiprocessor real-time scheduling taking into account preemption cost*, started January 2011, supervised by Yves Sorel.

PhD in progress: Manel Djemal, *Distributed real-time scheduling onto NoC architectures*, EDITE/UPMC, started Nov. 2010, co-supervised by Alix Munier (UPMC/Lip6) and D. Potop-Butucaru.

PhD in progress: Thomas Carle, *Real-time implementation of embedded control applications with conditional control onto time-triggered architectures*, EDITE/UPMC, started Sep. 2011, supervised by D. Potop-Butucaru.

PhD in progress: Pierre Courbin (ECE/UPEC), *Ordonnancement temps réel parallèle multiprocesseur*, started September 2009, supervised by Laurent George.

PhD in progress: Philippe Thierry (CIFRE Thales/UPEC), *Ordonnancement temps réel multiprocesseur sous contraintes de sécurité*, started April 2010, supervised by Laurent George.

PhD in progress: Vincent Sciandra, (CIFRE Veolia/UPEC), *Ordonnancement temps réel à criticité mixte dans les systèmes de transports intelligents (ITS)*, started Oct. 2010, supervised by Laurent George.

PhD in progress: Manar Qamhieh, (UPEMLV), *Ordonnancement temps réel de graphes de tâches parallèles à criticité mixte*, started Sept. 2010, co-supervised by Serge Midonnet (UPEMLV) and Laurent George.

PhD: Abdelhafid Mazouz, *An Empirical Study of Program Performance of OpenMP Applications on Multicore Platforms*, defended December 11 2012, UVSQ, supervised by Sid Touati (as part of his activities prior to joining Aoste), co-supervisd by D. Bartou (LABRI).

9.2.3. Juries

Robert de Simone

PhD reviewer: Sébastien Guillet (Université Bretagne-Sud), Cédric Auger (Université Orsay Paris-Sud),

HDR examiner: Ludovic Apvrille (Institut Mines-Telecom) (President of Jury).

Frédéric Mallet

PhD reviewer: Boutheina Bannour (Ecole Centrale Paris), Daniel Knorreck (Télécom ParisTech), Michel Lauer (INP Toulouse), Sabir Idrees (Télécom ParisTech)

PhD examiner: Cyril Faucher (Université de La Rochelle)

Sid Touati

PhD reviewer: Mohamed Benazouz (U. Paris 6), Jingyan Jourdan-Lu (ENS Lyon), Jean-Noël Quintin (INP Grenoble)

PhD examiner: Julien Jaegger (UVSQ)

Laurent George

PhD reviewer: Aurélien Monot (Université de Lorraine, Nancy)

Yves Sorel

PhD examiner: Mohamed Benazouz (University Pierre et Marie Curie)

Julien Deantoni

PhD examiner: Abderraouf Benyahia (Supelec)

<p style="text-align:center">**CONVECS Team**</p>

9. Dissemination

9.1. Scientific Animation

9.1.1. Software Dissemination and Internet Visibility

The CONVECS team distributes several software tools: the CADP toolbox (see 5.1), the TRAIAN compiler (see 5.2), and the PIC2LNT translator (see 5.3). In 2012, the main facts are the following:

- We prepared and distributed 11 successive beta-versions (from 2010-h to 2010-m, from 2011-a to 2011-c, and from 2012-a to 2012-b "Zurich") of CADP.
- We were requested to grant CADP licenses for 1227 different computers in the world.
- We released version 2.7 of the TRAIAN compiler for LOTOS NT in November 2012.
- We released version 2.0 of the PIC2LNT translator from an applied π-calculus to LNT in October 2012.

We constructed the CONVECS Web site (see http://convecs.inria.fr) and we updated it with scientific contents, announcements, publications, etc.

By the end of December 2012, the CADP forum (see http://cadp.inria.fr/forum.html), opened in 2007 for discussions regarding the CADP toolbox, had over 230 registered users and over 1400 messages had been exchanged.

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:

- Formal modeling and verification of BPEL-based Web service composition [62],
- A specific-domain design tool for FPGA-based image and video processing system [63],
- Quantitative timed analysis of interactive Markov chains [49],
- Synchronizability for verification of asynchronously communicating systems [31],
- Deciding choreography realizability [30],
- Automata learning through counterexample guided abstraction refinement [26],
- The Reo+mCRL2 framework for model-checking dataflow in service compositions [52],
- The IDCM analysis tool for components and architectures dedicated to incremental construction [54],
- Rigorous development of composite grid services [60],
- Integrating model-based testing and analysis tools via test case exchange [28], and
- The DFTCalc tool for calculating the failure probability of a dynamic fault tree (DFT) using LNT [61].

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

- Learning and testing the bounded retransmission protocol [27],
- Specification and validation of a real-time simple parallel kernel for dependable distributed systems [40],
- Abstraction-based malware analysis using rewriting and model checking [32], and
- Model checking of scenario-aware dataflow [58].

9.1.2. Program Committees

In 2012, the members of CONVECS took on the following responsibilities:

- H. Garavel is an editorial board member of STTT (Springer International Journal on Software Tools for Technology Transfer).
- F. Lang was a program committee member for NEPTUNE'2012 (Nice Environment with a Process and Tools Using Norms and Example), Paris, France, June 6-7, 2012.
- F. Lang was a program committee member for ESOCC'2012 (European Conference on Service-Oriented and Cloud Computing), Bertinoro, Italy, September 19-21, 2012.
- F. Lang and G. Salaün were program committee members for FMICS'2012 (17h International Workshop on Formal Methods for Industrial Critical Systems), Paris, France, August 27-28, 2012.
- R. Mateescu was a program committee member for GRAPHITE'2012 (1st International Workshop on Graph Inspection and Traversal Engineering), Talinn, Estonia, March 31 - April 1st, 2012.
- R. Mateescu was a program committee member for TASE'2012 (6th International Symposium on Theoretical Aspects of Software Engineering), Beijing, China, July 4-6, 2012.
- G. Salaün is an editorial board member of SOCA (Springer International Journal on Service Oriented Computing and Applications).
- G. Salaün was a program committee member for COORDINATION'2012 (14th International Conference on Coordination Models and Languages), Stockholm, Sweden, June 14-15, 2012.
- G. Salaün was a program committee chair for FACS'2012 (9th International Symposium on Formal Aspects of Component Software), Mountain View, USA, September 12-14, 2012.
- G. Salaün was a program committee member for FLACOS'2012 (6th International Workshop on Formal Languages and Analysis of Contract-Oriented Software), Bertinoro, Italy, September 19, 2012.
- G. Salaün was a steering committee member for FOCLASA'2012 (11th International Workshop on Foundations of Coordination Languages and Self-adaptation), Newcastle upon Tyne, UK, September 8, 2012.
- W. Serwe was a program committee member for PDMC'2012 (11th International Workshop on Parallel and Distributed Methods in Verification), Imperial College, London, UK, September 17, 2012.

9.1.3. Awards and Distinctions

- H. Garavel is an invited professor at the University of Saarland (Germany) after he received the Gay-Lussac Humboldt Prize in 2011.
- M. Güdemann received the Software Engineering Award of the Ernst Denert Association in 2012.

9.1.4. Lectures and Invited Conferences

- H. Garavel gave a keynote lecture entitled "*Three Decades of Success Stories in Formal Methods*" at FMICS'2012 (Paris, France) on August 28, 2012.
- H. Garavel gave a lecture entitled "*Trois décennies de réussite en méthodes formelles*" in the Aerospace Valley industrial conference on formal methods (Toulouse, France) on November 13, 2012.
- M. Güdemann visited the Institute for Systems and Systems Engineering (ISSE) at the University of Augsburg (Germany) on March 1st, 2012. He gave a tutorial on CADP.
- F. Lang and W. Serwe presented a tutorial on CADP at AFADL'2012 (Grenoble, France) on January 12, 2012.
- R. Mateescu visited the LRI laboratory (University Paris-Sud at Evry) on March 21–22, 2012. He gave a talk entitled "*Extending Temporal Logics in Practice: Model Checking and Applications*" on March 22, 2012.

- R. Mateescu presented a tutorial on CADP at FM'2012 (Paris, France) on August 28, 2012.
- R. Mateescu gave a talk entitled "*Querying Graphs On-the-Fly using a Model Checking Language*" at the LIG laboratory (Grenoble) on September 27, 2012.
- G. Salaün visited the LRI laboratory (University Paris-Sud at Evry) on March 19, 2012. He gave a talk entitled "*Specifying and Verifying a Self-Configuration Protocol for Distributed Applications in the Cloud using LNT and CADP*" on March 19, 2012.
- G. Salaün visited the LINA laboratory (University of Nantes) on March 22–23, 2012. He gave a talk entitled "*Specifying and Verifying a Self-configuration Protocol for Distributed Applications in the Cloud using LNT and CADP*" on March 22, 2012.
- G. Salaün visited the FBK laboratory (Trento, Italy) on March 28, 2012. He gave a talk entitled "*Design and Verification of Distributed Systems*" on March 28, 2012.
- G. Salaün visited the IRIT laboratory (Toulouse) on November 19–21, 2012. He gave a talk entitled "*Design and Verification of Communicating Systems*" on November 19, 2012.
- W. Serwe participated to the kick-off meeting of the Sensation project, held on November 1–2, 2012 in Aalborg (Denmark). He gave a talk entitled "*Model Checking and Performance Evaluation with CADP Illustrated on Shared-Memory Mutual Exclusion Protocols*" on November 2, 2012.
- W. Serwe participated to the Grid'5000 winter school, held on December 3–6, 2012 in Nantes. He gave a talk entitled "*Large Scale Distributed Verification using CADP on Grid'5000*" on December 6, 2012.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

In 2012, we carried out the following teaching activities:

- H. Evrard served as a teaching assistant in a course on "*Algorithmique et structures de données*", given by Frédéric Wagner to the first year computer science engineering students of ENSIMAG (18 hours).
- H. Evrard served as a teaching assistant in a course on "*Introduction aux réseaux de communication*", given by Roland Groz to the first year computer science engineering students of ENSIMAG (18 hours).
- H. Evrard served as a teaching assistant in a course on "*Systèmes d'exploitation et programmation concurrente*", given by Yves Denneulin to the first year computer science engineering students of ENSIMAG (18 hours).
- H. Garavel created a block course entitled "*Advanced Concurrency Theory*" for the bachelor and master students of Saarland University (4 ECTS credits, assistant: Alexander Graf-Brill).
- A. Kriouile served as a teaching assistant in a course on "*Conception de circuits et architecture des ordinateurs*", given by Frédéric Pétrot to the first year computer science engineering students of ENSIMAG (18 hours).
- F. Lang and W. Serwe gave, jointly with Pascal Raymond (CNRS, Verimag), a course on "*Méthodes formelles de développement*" to the computer science engineering students of CNAM ("*Conservatoire National des Arts et Métiers*") Grenoble (27 hours).
- F. Lang and W. Serwe gave a course on "*Spécification et vérification de systèmes concurrents et temps-réel*" to the third year computer science engineering students of ENSIMAG (18 hours).
- G. Salaün gave lectures on "*Algorithmics and Object-Oriented Programming*" to the 2nd year computer science engineering students of ENSIMAG (36 hours).
- G. Salaün is co-responsible of the ISI (*Ingénierie des Systèmes d'Information*) department of ENSIMAG since September 1, 2011.

9.2.2. Juries

- G. Salaün was a panel member for Jose Antonio Martin Baena's PhD thesis, entitled "*Secure Adaptation of Software Services*", defended at the University of Málaga, Spain, on July 24, 2012.

- W. Serwe was a core committee / reading committee member of F. P. M. Stapper's PhD thesis, entitled "*Bridging Formal Methods: An Engineering Perspective*", defended at the Technical University of Eindhoven, The Netherlands, on November 8, 2012.

9.3. Popularization

H. Garavel participates to the committee in charge of organizing the Aerospace Valley series of industrial conferences on formal methods. The first conference, held on November 13, 2012, was a success, as it attracted 85 participants, among which 61 industrialists from 33 different companies.

R. Mateescu published a report about the 17th workshop on *Formal Methods for Industrial Critical Systems* [21].

In the context of the 20th anniversary of the Inria research center in Montbonnot, H. Garavel contributed to the collection of articles describing the evolution of computer sciences during the last 20 years [20].

9.4. Miscellaneous Activities

Within the Minalogic *Pôle de compétitivité mondial*, H. Garavel is a member of the operational committee of the EMSOC cluster (Embedded System on Chip).

H. Garavel was a reviewer for the German Excellence Initiative (Engineering Sciences Review Panel ING 14 for Clusters of Excellence), Bonn (Germany), January 10–12, 2012.

H. Garavel was a member of the working group in charge of restructuring the scientific themes of the LIG laboratory.

H. Garavel, F. Lang, R. Mateescu, G. Salaün, and W. Serwe attended the Inria evaluation seminar for teams working on "Embedded Systems and Real-Time", Rungis/Orly (France), March 19–20, 2012.

H. Garavel participated in the 40th Symposium for Research Award Winners of the Alexander von Humboldt Foundation, Bamberg (Germany), March 22–25, 2012.

H. Garavel participated in the "Cérémonie de remise du Prix Gay-Lussac Humboldt 2011", Académie des Sciences – Institut de France, Paris, April 10, 2012.

H. Garavel participated in the Annual Meeting (*Jahrestagung*) of the Alexander von Humboldt Foundation, Berlin, June 19–21, 2012.

H. Garavel was a reviewer for the "*Futur et Ruptures*" joint programme of Institut Mines-Télécom and Fondation Télécom.

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

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

G. Salaün was a member of the council of ENSIMAG until October 2012.

G. Salaün is a member of the council of the LIG laboratory.

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

<div align="center">

DART Project-Team

</div>

9. Dissemination

9.1. Scientific Animation

Samy Meftali was member of the program committee of:

- Conference on Design and Architectures for Signal and Image Processing. DASIP 2012. October 23-25, 2012. Karlsruhe, Germany
- International Conference on EMBEDDED SYSTEMS in TELECOMMUNICATIONS and IN-STRUMENTATION, 5-7 novembre 2012, Annaba. Algeria.
- The International Symposium on System-on-Chip Tampere, Finland. October 11-12, 2012.

Vlad Rusu was member of the program committee of the IFIP Joint International Conference on Formal Techniques for Distributed Systems (FMOODS & FORTE 2012).

9.1. Teaching - Supervision - Juries

9.1.1. Teaching

Licence : Frédéric Guyomarch, Algorithmics and programming, 70h, L1, Université Lille 1, France

Licence : Frédéric Guyomarch, Data structures, 50h, L1, Université Lille 1, France

Licence : Frédéric Guyomarch, Architecture, 30h, L1, Université Lille 1, France

Licence : Frédéric Guyomarch, Graph theory, 40h, L2, Université Lille 1, France

Master : Frédéric Guyomarch, Advanced achitectures, 30h, M1, Université Lille 1, France

Licence : Samy Meftali, Architectures élémentaires, 90h eqTD, L2, Université Lille 1, France

Licence : Samy Meftali, Architecture, 40h, L3, Université Lille 1, France

Master :Samy Meftali, Architectures évoluées, 68h, M1, Université Lille 1, France

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

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

Master: Philippe Marquet, Design of Operating System, 42h, M1, Université Lille 1, France

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

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

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

Licence : Vlad Rusu, Architectures élémentaires, 30h, L2, Université Lille 1, France

Master : Vlad Rusu, Introduction to Formal Verification with PVS, 20h, M2, Universidad Complutense de Madrid, Espagne

9.1.2. Supervision

PhD : Wendell Rodrigues, *Une Méthodologie pour le Développement d'Applications Hautes Performances sur des Architectures GPGPU: Application à la Simulation des Machines Éléctriques*, Université de Lille 1, 26-01-2012, Frédéric Guyomarch and Jean-Luc Dekeyser

9.1.3. Juries

Frédéric Guyomarch was the external examiner for Jing Guo's PhD (University of Hertfordshire, UK). entitled *Fully Automated Transformation of Hardware-Agnostic, Data-Parallel Programs for Host-Driven Executions on GPUs*.

Vlad Rusu was on the PhD commitee of Michaël Lauer (Université de Toulouse) entitled *Une méthode globale pour la vérification d'exigences temps réel Application à l'Avionique Modulaire Intégrée*

Samy Meftali was on the PhD commitee of Yaset OLIVA VENEGAS(INSA Rennes) entitled *High Level Modeling of Run-Time Managers for the Design of Heterogeneous Embedded Systems*

Samy Meftali was on the PhD commitee of Amine Anane(Univ. Montréal) entitled *Application du concept des transactions pour la modélisation et la simulation multicoeur des systèmes sur puce*

9.2. Popularization

Pamela Wattebled is chair of the organizing comitee of Majecstic 2012. MajecSTIC 2012 is the 9th edition of the conference MajecSTIC. This conference is organized by young researchers. This year it takes place in Lille and organized by Pamela WATTEBLED-MEFTALI (project-team DART), Nicolas GOUVY (project-team FUN) and Adel NOUREDDINE (project-team ADAM).

<p style="text-align:center">**ESPRESSO Project-Team**</p>

8. Dissemination

8.1. Scientific Animation

8.1.1. Invited Lectures

Jean-Pierre Talpin gave a series of invited lectures on synchronous programming and on Polychrony at the Ecole Centrale de Pékin and at Beihang University, May 2012, in Beijing, China.

Jean-Pierre Talpin was invited at the 2012 ACM/IEEE Conference on Logic in Computer Science, in June 2012, Dubrovnik, to receive the ACM/IEEE LICS Test of Time Award. He gave a short presentation on the technical challenges and theoretical breakthroughs of his awarded paper: "A type and effect discipline", with his co-author Pierre Jouvelot.

Jean-Pierre Talpin participated to the Dagstuhl meeting on Architecture-Driven Semantic Analysis of Embedded Systems in June 2012, and presented the tools developped by ESPRESSO for co-modeling embedded software architectures with Polychrony.

Jean-Pierre Talpin gave an invited presentation on extending AADL with a timed annex at the AADL standardisation committee and SAE conference, October 2012 in Phoenix, a followup of which is the definition by the ESPRESSO project-team of a synchronous annex for AADL.

8.1.2. Conferences

Jean-Pierre Talpin is a member of the steering committee of the ACM-IEEE conference on methods and models for co-design (MEMOCODE) and of the editorial board of the EURASIP Journal on Embedded Systems. He served as technical program committee member for the following conferences:

 HLDVT'11 http://www.hldvt.com/11
 SAC'11 http://www.acm.org/conferences/sac/sac2011
 SIES'11 http://www.mrtc.mdh.se/sies2011

Jean-Pierre Talpin co-organized with Elisabeth Lebret the 19th. edition of the synchronous programming workshop, held in Le Croisic, November 2012 (http://synchron2012.inria.fr).

Thierry Gautier served as technical program commitee member for the conference ESLsyn 2012 (http://www.ecsi.org/eslsyn2012) and MEMOCODE 2012 (http://memocode.irisa.fr/2012/MEMOCODE%202012.html).

8.2. Teaching - Supervision - Juries

8.2.1. Juries

Jean-Pierre Talpin served as referee and president at the thesis defense of Mikel Cordovilla, entitled "Environnement de développement d'applications multi-périodiques sur plateforme multi-cœur: la boîte à outils SchedMCore", held on April 2, 2012 at ONERA.

Paul Le Guernic served as examiner at the Habilitation thesis defense of Abdoulaye Gamatié, entitled "Design and analysis for multi-clock and data-intensive applications on multiprocessor systems-on-chip", held on November 15, 2012 at Université de Lille 1. He served also as referee at the thesis defense of Michaël Lafaye, entitled "Modélisation de plate-forme avionique pour exploration de performance en avance de phase", held on November 19, 2012 at Télécom ParisTech.

Jean-Pierre Talpin served on the Professor selection committee of ENSEEIHT in May 2012.

Thierry Gautier served on an Associate Professor selection committee of Université de Rennes 1 in May 2012.

Loïc Besnard served as president in a jury for the competitive selection of engineers at CNRS in October 2012.

Paul Le Guernic served as "rapporteur" of Inria Research Center Rennes - Bretagne-Atlantique at the Regional symposium of Higher Education and Research (Assises territoriales de l'enseignement supŕieur et de la recherche) in Nantes and Rennes.

MUTANT Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Community Initiatives

The Brillouin Seminar series on *Information Geometry* is coordinated by MUTANT in partnership with LIX and THALES. It gathers 80 international researchers on the topic from various disciplines. In 2012, we organized 6 talks. Videos are available on the seminar website.

Jean-Louis Giavitto is the management team of the GDR GPL (Génie de la programmation et du logiciel), responsible with Etienne Moreau of the "Languages and Vérification" pole of the GDR. He is also and expert for the ANR DEFI projects and a reviewer for FET projets for the UC.

8.1.2. Editorial Boards

Jean-Louis Giavitto is the redactor-in-chief of TSI (Technique et Science Informatique), a french scientific journal published by Lavoisier and Hermes Science.

8.1.3. Participation in Program Committees of Conferences

Florent Jacquemard has been member of the program committees of the 6th International Joint Conference on Automated Reasoning (IJCAR 2012), June 26th to July 1st, 2012, Manchester, UK, and of the International Workshop on Trends in Tree Automata and Tree Transducers (TTATT 2012), a satellite workshop of the 23rd International Conference on Rewriting Techniques and Applications (RTA 2012), June 2, 2012, Nagoya, Japan.

Jean-Louis Giavitto was co-chair of the Spatial Computing Workshop (SCW2012) a satellite workshop of AAMAS, 5 June 2012, Valencia, Spain. He was also member of the Program Committees of: AFADL 2012 (Approches Formelles dans l'Assistance au Développement de Logiciels, 11-13 January 2012, Grenoble), IPCAT 2012 9th International Conference on Information Processing in Cells and Tissues 31st March – 2nd April 2012, Trinity College, Cambridge, GDS track at GECCO 2012, the Generative and Developmental track at the Genetic and Evolutionary Computation Conference, 7–11 July 2012, Philadelphia, FHIES 2012 Foundations of Health Information Engineering and Systems, an international symposium co-located with FM 2012, August 27-28, Paris, MeCBIC 2012, 6th Workshop on Membrane Computing and Biologically Inspired Process Calculi 8th September 2012, Newcastle.

8.1.4. Participation in Conferences

- José Echeveste, Jean-Louis Giavitto and Florent Jacquemard attended the 2012 International Computer Music Conference (Ljubljana, Slovenia, 9-14 September) and gave a talk on fault tolerance and language extensions of *Antescofo* [15].
- Jean-Louis Giavitto attended the:
    - Journées du GDR GPL (comité de direction)
    - SCW 2012, Valencia Spain, 5 June 2012 (chair)
    - UCNC 2012, Orleans and gave a tutorial on MGS

8.1.5. Invited Talks

Arshia Cont gave an invited talk at the Computer-Human Interactive Performance Symposium in University City London (UCL) in June 2012.

Arshia Cont and Jean-Louis Giavitto gave an invited talk in the Produce Time Symposium in June 2012 at IRCAM.

Jean-Louis Giavitto:

- tutorial on MGS at the 11th International Conference Unconventional Computation and Natural Computation UCNC 2012, 37 September, Orléans.
- *Non-Standard Multiset*, for the mini symposium Let's Imagine the Futur for the retirement of Jean-Pierre Banâtre, 7–8 Novembre, Rennes.
- *Programmation spatiale : application à l'analyse des contes de fées et à l'analyse musicale*, IPAC seminar, 8th March, Nancy.
- *Le projet AutoChem*, presentation closing the ANR Blanc project, at the NAR Symposium, January 2012.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence :
- Arshia Cont, Audio Technology Review, 2h/week, 3rd year Bachelors, Conservatoire Nationale Supérieure de la Musique et de la Danse de Paris (CNSMDP), Métier du Son, Paris, France.

Master :
- Arshia Cont, Machine Learning for Music, 18h, Master ATIAM, Université Pierre et Marie Curie (UPMC), Paris, France.

8.2.2. Supervision

PhD : Arnaud Dessein, *Computational methods of information geometry with real-time applications in audio signal processing*, Université Pierre et Marie Curie (UPMC), December 2012, Arshia Cont (co-directed with Gérard Assayag, IRCAM).

PhD in progress :
- José Echeveste, Synchronous Languages for Computer Music Composition and Performance, Started September 2011, co-directed by Jean-Louis Giavitto and Arshia Cont.

8.2.3. Juries

- Arshia Cont participated in the defense committee for Augustin Lefèvre, "Dictionary learning methods for single-channel audio source separation", ENS Cachan, September 2012.
- Arshia Cont participated in the defense committee for Mauricio Toro, "Structured Interactive Scores", University of Bordeaux 1 (LaBRI), September 2012.
- Florent Jacquemard was a examinator for the PhD of Hèdi Benzina, "Enforcing Virtualized Systems Security", ENS Cachan (LSV), December 2012.
- Jean-Louis Giavitto was a reviewer for the thesis of:
  - Héctor Fernández, "Flexible Coordination through the Chemical Metaphor for Service Infrastructures", University of Rennes 1 (IRISA), June 2012.
  - Jose David Fernández Rodríguez, "The Evolution of Diversity in the Structure and Function of Artificial Organisms", Universidad de Maálaga, Spain, January 2012.

8.3. Popularization

8.3.1. Cultural Events, Highlights

The Antescofo software developed and maintained by the team, has been featured in various prestigious international events with the following highlights:

- 13 World-premiers for live electronics and instruments by international composers such as Kaija Saariaho, Philippe Manoury, Steve Coleman and Marco Stroppa including one opera. See complete list.
- More than 30 world-class public performances around the world including: Antescofo premier with *New York Philharmonics* (June 2012), Lucerne Festivale (August 2012), Salle Pleyel (September 2012), Warsaw Autumn Festival (September 2012), Royal Albert Hall in London (August 2012), Vienna Festwochen (June 2012), Opéra Comique de Paris (June 2012), and more.

See partial list.

- Two Giga-Hertz Prizes for two pieces strongly featuring *Antescofo* (life-time award for Emmanuel Nunes' *Einspielung*, young category for Lara Morciano).
- A documentary movie on Antescofo produced by Inria. (watch)

8.3.2. International Public Press

BBC Radio program featuring *Antescofo* on the occasion of a live performance in Royal Albert Hall.

8.3.3. National Public Press

Major public press mentions for *Antescofo* in 2012:

- *Antescofo: Au plus près de la partition*, Science et Avenir, July 2012.
- *L'ordinateur qui joue comme un musicien*, La recherche, June 2012.
- Quand l'informatique maîtrise le temps de l'interprétation musicale, France Culture Online , July 2012.
- Antescofo à l'avant-garde de l'informatique musicale, InterStices, November 2012.
- Sous le signe du calcul (with F. Reichenmann) in DocSciences, special issue on " Alan Turing : la pensée informatique" (DocSciences is a journal for college students published by the Rectorat de Versailles), June 2012. Published also on the InterStices web site, September 2012.
- À propos des nouveaux langages de programmation, audio podcast, InterStices, July 2012.

8.3.4. Exhibitions

- The *MuTant* team's *Antescofo* software was the demo feature for Inria's stand at the 13th exhibition for Mathematical Cultures and Games (Salon cultures et jeux mathématiques) in June 2012.
- *MuTant* members hold a stand during the "Fêtes de la science" on *Antescofo* at Inria Rocquencourt in October 2012.
- Jean-Louis Giavitto has participated to a public debate of the Bar des Sciences with G. Longo and G. Dowek on "Turing aurait 100 ans – De Turing au Qbit", 7th November.
- Jean-Louis Giavitto has participated to a public debate following the projection of Codebreaker: Alan Turing with C. Villani, B. Chazelle and J. Lassègue at the movie theater Grand Action, 17th December.

PARKAS Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Event organization

- J. Vuillemin is member of the International Scientific Advisory Board of the National ICT Australia.
- J. Vuillemin chairs the Scientific Advisory Board of the national Institute for InfoCom Research I2R in Singapore.
- F. Zappa Nardelli is member of the "comité executif" of the CEA-EDF-Inria summer schools.
- F. Zappa Nardelli served in the POPL 2012 ERC.
- F. Zappa Nardelli is member of the "comité de suivi doctoral" de l'Inria Saclay.
- A. Cohen is the General Chair of the 7th HiPEAC conference, January 2012. Louis Mandel is member of the local arrangements committee. The conference pionneered a new "journal first" publication model, and has been completely reorganized into a large networking event with 27 parallel events, an industry exhibit with 50 companies booths and posters, and a European project exhibit with 46 projects from the computing systems, embedded systems strategic objectives of the FP7 and from the FET programme. 516 registered participants, 34 ACM TACO journal papers presented (the record number for previous HiPEAC conferences was 210 participants).
- M. Pouzet is in charge, with Catherine Dubois (IIE CNAM, Evry) of the national research group LTP (Language, Types, Proofs) of the French GDR GLP ("Génie de la Programmation et du Logiciel"). Two meetings a year with three invited speakers.
- M. Pouzet organised 18th edition of SYNCHRON (http://synchron2011.di.ens.fr), the workshop on Synchronous Programming and Applications, in Dec. 2011 in Damaries-les-lys. We got the record track of 80 participants and a special half-day devoted to synchronous programming for music applications with collegues from IRCAM.

9.1.2. Editorial boards

- Jean Vuillemin is on the board of 5 international journals.
- Marc Pouzet is associate editor of the EURASIP Journal on Embedded systems (http://jes.eurasipjournals.com.
- Marc Pouzet is "directeur de collection" for Hermes publisher.
- Albert Cohen is on the editorial board of the International Journal on Parallel Programming (IJPP, http://www.springer.com/computer/theoretical+computer+science/journal/10766).
- Albert Cohen is on the distinguished reviewer board of the ACM Transactions on Architecture and Code Optimization (TACO).

9.1.3. Program committees

- M. Pouzet is a member of the program committee of the following conferences: Design, Automation & Test in Europe (DATE 2012); Embedded Software (EMSOFT 2012); Complex Systems Design & Management (CSD&M) 2012; Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL 2012); ACM Conf. on the Principles and Applications of Declarative Programming (PADL 2012), located with POPL;
- M. Pouzet is an expert reviewer for the Design Automation Conference (DAC) in 2012 and 2013.
- A. Cohen is the chair of the DAC 2013 ESS1 TPC subcommittee, and was the co-chair of the DAC 2012 ESS1&2 TPC subcommittee.

- A. Cohen is the program chair of ETAPS CC 2014.
- A. Cohen is a member of the program committee of the following conferences: ICS 2012, ETAPS CC 2013, PPoPP 2013 external review committee.
- A. Cohen is the co-general chair of the ICPP-EMS 2013 workshop (with ICPP).
- A. Cohen is a member of the program committee of the following workshops: IMPACT 2012 and 2013 (with HiPEAC), HiRES 2013 (with HiPEAC), GPGPU 2012 and 2013 (with ASPLOS), COSMIC 2013 (with CGO), PLC 2012 and 2013 (with IPDPS), ICPP-EMS 2012 (with ICPP).
- L. Mandel, member of the program committee of the Journées Francophones des Langages Applicatifs (JFLA 2012).

9.1.4. Invited Presentations

- A. Cohen was a keynote speaker at the IMPACT 2013 workshop (with HiPEAC) "Adopt a Polyhedral Compiler!", July 2011.
- A. Cohen gave an invited presentation at AMD Bangalore titled "Languages and Compilers for Productivity and Efficiency", June 2012.
- A. Cohen gave a Priti Shankar seminar at the Indian Institute of Science, CSA department, titled "Polyhedral Compilation Off the Beaten Path", June 2012.
- M. Pouzet gave an invited presentation at the Int. Conference on Complex Systems, Design & Management (CSDM), Dec. 2011.
- M. Pouzet gave an invited presentation at the "Séminaire MaMux", IRCAM, Paris. Feb. 2012.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: "Systèmes" (L3), L. Mandel (42h), Université Paris-Sud 11, France

Licence: "Systèmes et réseaux" (L3), M. Pouzet (24h), L. Mandel (24h), École Normale Supérieure, France

Licence: "Langages de programmation et compilation" (L3), L. Mandel (24h), École Normale Supérieure, France

Master Parisien de Recherche en Informatique (MPRI): "Synchronous systems" (M2), M. Pouzet (12h), J. Vuillemin (6h), L. Mandel (6h), École Normale Supérieure and Université Paris Diderot, France

Licence: "From Algorithm to Circuit" (L3), J. Vuillem (64h), École Normale Supérieure, France

Master Parisien de Recherche en Informatique (MPRI): "Semantics and tools for multicore programming" (M2), A. Cohen (9h), F. Zappa Nardelli (13.5h), École Normale Supérieure and Université Paris Diderot, France

Marc Pouzet is "responsable du concours d'entrée à l'ENS", for the Computer Science department (since Sept. 2010).

Marc Pouzet is director of studies (directeur des études) of the Computer Science department (since Sept. 2012).

9.2.2. Supervision

M2: R. Morisset (ENS), Correctness of optimisations in the C11/C++11 memory model, september 2012;

M2: P. Pawan (IIT Kanpur, India), Hunting concurrency compiler bugs, september 2012;

M2: F. Gindraud (ENS Lyon), definition, code generation, and formal verification of a software controlled cache coherence protocol;

M2: B. Arnoux (École Polytechnique, Telecom ParisTech), globally adressable memory model for data-flow execution.

M1: C. Lecourt (École Polytechnnique), numerical receipies and examples for Zélus.

M2: G. Baudart (École normale supérieure, Cachan), A synchronous semantics and implementation for Antescofo.

9.2.3. Juries

- A. Cohen was a reviewer of the following PhD theses: Nicolas Benoit (January 2012, Université de Versailles St-Quentin), Artur Pietrek (October 2012, Université Joseph Fourier), Mehdu Amini (November 2012, MINES ParisTech), Selma Saidi (November 2012, Université Joseph Fourier), Dmitry Nadezhkin (December 2012, Leiden University, The Netherlands).

- A. Cohen was a committee member of the following PhD theses: Delphine Demange (October 2012, École Normale Supérieure de Cachan – Université Européenne de Bretagne), Quentin Colombet (December 2012, École Normale Supérieure de Lyon).

- A. Cohen was a committee member of the following Habilitation theses: Gaël Thomas (December 2012, Université Pierre et Marie Curie), Cédric Bastoul (December 2012, Université Paris Sud).

- M. Pouzet was the President of the following PhD. thesis: Peter Schrammel (October 2012, Université de Grenoble).

9.3. Popularization

- L. Mandel and M. Pouzet, were invited to give a lecture at IRCAM in the Master of "Acoustique, Traitement du signal, Informatique, Appliqués à la Musique". Nov. 2010, Nov. 2011, and Nov. 2012.

<div align="center" style="color:red">

POP ART Project-Team

</div>

9. Dissemination

9.1. Scientific Animation

- Pascal Fradet served in the program committee of JFLA 2013 (*v*ingt quatrièmes Journées Francophones des Langages Applicatifs).
- Gregor Goessler served in the program committees of the international conference DATE 2013.
- Bertrand Jeannet was Program Chair of the TAPAS workshop (Tools for Automatic Program AnalysiS) affiliated to SAS (Static Analysis Symposium), that was held in Deauville in September 2012.
- Alain Girault served in the program committees of the international conferences DAC 2012, MEMOCODE 2012, LCTES 2012, and APSIPA ASC 2012,

9.2. Teaching - Supervision - Juries

9.2.1. Supervision

PhD in progress: Vagelis Bebelis, "Advanced dataflow programming for embedded systems", Grenoble University, since 12/2011, co-advised by Pascal Fradet and Alain Girault.

PhD in progress: Dmitry Burlyaev, "Specification and synthesis of fault-tolerant circuits", Grenoble University, since 12/2011, co-advised by Pascal Fradet and Alain Girault.

PhD in progress: Gideon Smeding, Grenoble University, "Distribution of synchronous programs withe respect to real-time constraints", co-advised by Gregor Goessler and Joseph Sifakis since 12/2009.

PhD : Peter Schrammel, "Logico-numerical verification methods for discrete and hybrid systems", Grenoble University, defended on 18/10/2012, co-advised by Alain Girault and Bertrand Jeannet

9.2.2. Juries

- Bertrand Jeannet was examiner for the PhD of Romain Testylier (University of Grenoble).
- Alain Girault was referee for the PhD thesis of Aurélien Monot (University of Lorraine), president of the PhD jury of Slim Bouguerra (University of Grenoble), and president of the PhD jury of Christophe Junke (University of Orsay).

8. Dissemination

8.1. Scientific Animation

Eric Badouel is the secretary of the steering committee of CARI, the African Conference on Research on Computer Science and Applied Mathematics. He took part in the programme committee and in the organizing committee of CARI 2012. He is a member of the editorial board of the ARIMA Journal.

Albert Benveniste is associated editor at large (AEAL) for the journal *IEEE Trans. on Automatic Control*. He is member of the Strategic Advisory Council of the Institute for Systems Research, Univ. of Maryland, College Park, USA. He belongs to the Scientific Advisory Board of INRIA, where he is in charge of the area of Embedded Systems. [1]

Benoît Caillaud has served in the steering and program committees of the International Conference on Application of Concurrency to System Design (ACSD 2012). He is serving on the Evaluation Committee of INRIA.

Philippe Darondeau has served on the program committees of the 23rd International Conference on Concurrency Theory (CONCUR 2012) and 11th International Workshop on Discrete Event Systems (WODES 2012). He is a member of the IFIP Working Group WG2.2 and has served as secretery of this working group until September 2012.

Sophie Pinchinat is serving in the editorial board of the Journal on Discrete Event Dynamic Systems, Theory and Applications. She has served on the program committee of the 10th Conference on Logic and the Foundations of Game and Decision Theory (LOFT 2012).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

- Benoit Caillaud has contributed to the training programme for the computer-science option of the *agregation* in mathematics, at ENS Cachan-Ker Lann.
- Sophie Pinchinat has contributed to three courses on verification and game theory in the computer science master degree of the University of Rennes 1 and at Supelec. She has taught algorithmics at undergraduate level at the university of Rennes 1. She has taught embedded systems design in the engineering degree of the university of Rennes 1.

8.2.2. Supervision

Several PhDs are in progress:
- Lamine Diouf, *Artefact opacity in workflow systems*, started in 2010, supervised by Eric Badouel.
- Bastien Maubert, *Logical Foundations of Imperfect Information Games*, started September 2010, co-supervised by Sophie Pinchinat and Guillaume Aucher.
- Stéphanie Georges, *Formal approaches to physical security analysis: Attack tree synthesis*, started December 2011, co-supervised by Sophie Pinchinat and Achour Mostefaoui.

8.2.3. Juries

Sophie Pinchinat has served on the PhD thesis jury of Loïg Jézeéquel (project-team DISTRIBCOM).

---

[1]Only facts related to the activities of Team S4 are mentioned. Other roles or duties concern the DistribCom team, to which A. Benveniste also belongs.

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

9. Dissemination

9.1. Scientific Animation

- Liliana Cucu is the Delegate of International Relations for the Inria Nancy-Grand Est center.
- Olivier Zendra is an elected member of the Research Center Committee of Inria Nancy Grand Est.
- Nicolas Navet chairs with Thomas Nolte (MRTC Mälardalen) of the Sub-Committee on Real-Time Fault Tolerant Systems of the IEEE Industrial Electronic Society (IES) - Technical Committee on Factory Automation (TCFA).
- Nicolas Navet is member of the Editorial Board of the Journal of Embedded Computing (IOS Press).
- Liliana Cucu is an elected member of Inria Evaluation Commission (CE).
- Olivier Zendra is head of the Documentation Committee of Inria Nancy Grand Est, member of the Health, Safety and Work Environment of Inria and of Inria Nancy Grand Est - LORIA Committees, member of the Permanent Education Committee of Inria Nancy Grand Est - LORIA, member of the new Sustainable Development Local and National Committees, member of the Inria Nancy Grand Est - LORIA Committee for the selection of hardware configurations.
- Olivier Zendra is CIR expert for the Ministry of Research for the scientific evaluation of research in companies.
- Liliana Cucu and Nicoals Navet are ANRT expert for evaluating CIFRE applications.
- Olivier Zendra is founder and steering committee member of the ICOOOLPS (International Workshop on Implementation, Compilation, Optimization of Object-Oriented Languages, Programs and Systems) workshop.
- Liliana Cucu and Nicolas Navet were general chairs of the 20th International Conference on Real-Time and Network Systems (RTNS 2012).
- Liliana Cucu was co-chair of RTSOPS and WIP session of WFCS 2012.
- Liliana Cucu was program committe member of ECRTS, ETFA, SIES, ACM RACS.
- Nicolas Navet was program committe member of ACM RACS'2012, IEEE RSP'2012, Track on Industrial Communication Systems and Real-Time and (Networked) Embedded Systems at IEEE ETFA 2012, IEEE ICESS-2012, IEEE SIES'2012, IEEE WFCS'2012, WoNeCa-2012.
- Nicolas Navet was co-animator of the High Performance Embedded Systems (HPES) cluster of GDR CNRS ASR, and co-animator of Actriss group (real-time services and infrastructure) of HPES cluster.
- Olivier Zendra was co-chair of ICOOOLPS 2012, June 11th, Beijing, CN.
- Olivier Zendra was program committee member for CIEL 2012, DASIP 2012, ICOOOLPS 2012, RESoLVE 2012.
- The permanent members of TRIO team are reviewers for numerous international Conferences and Workshops and, in particular for the following journals: IEEE Transactions on Industrial Informatics, Real-Time Systems, IEEE Computer Communications, Journal of Discrete Event Systems, Journal of Systems Architecture, Journal of Embedded Computing, Journal of Scheduling, Theoretical Computer Science, ACM Surveys, ACM Transactions on Embedded Computing Systems, Information Processing Letters.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence : Olivier Zendra, langages à objets / Java, 53h, niveau (L2), University of Lorraine, France

Master : Liliana Cucu, Multiprocessor real-time systems, 30h, niveau (M1), University of Lorraine, France

Master : Nicolas Navet, Real-time critical systems, 30h, niveau (M1), University of Lorraine, France

9.2.2. Supervision

PhD & HdR :

PhD : Aurélien Monot, Vérification des contraintes temporelles de bout-en-bout dans le contexte AutoSar, University of Lorraine, November 29th, Françoise Simonot, Nicolas Navet and Bernard Bavoux

PhD : Pierre Caserta, Analyse statique et dynamique de code et visualisation des logiciels via la métaphore de la ville: contribution à l'aide à la compréhension des programmes, December 7th, Jean-Pierre Thomesse and Olivier Zendra

PhD in progress: Dorin Maxim, Probabilistic real-time systems, October 1st 2010, Liliana Cucu and Françoise Simonot-Lion

9.2.3. Juries

- Liliana Cucu was member of the PhD thesis jury of Mikel Cordovilla, defended in April 2012 at ONERA, Toulouse.
- Olivier Zendra was member of the PhD thesis jury of Olivier Sallenave, defended in November 2012 at LIRMM / Université de Montpellier

VERTECS Project-Team

8. Dissemination

8.1. Scientific Animation

Nathalie Bertrand   was PC member of QAPL'12, QEST'12, Infinity'12 and SYNT'12. She is since september 2012 a Steering Committee member of QEST. She was invited to give a talk at the research seminar of the Quantitative Logics and Automata (QuantLA) Doctoral School in Dresden, in December 2012. She is also a member of the panel for the Gilles Kahn prize awarded each year to an excellent PhD thesis in computer science.

Thierry Jéron   is Vice President of the Project Committee of Inria Rennes - Bretagne Atlantique. He is member of the IFIP Working Group 10.2 on Embedded Systems. He is a member of the Steering Committe of the School MOVEP (held in Marseille in December 2012), and PC member of ICFEM 2012, ICST 2012, ICTSS 2012, RV 2013, TAP 2012 and 2013. He gave a lecture at the Summer School TAROT 2012. He co-organizes the Dagstuhl Seminar 13021 on "Symbolic Methods in Testing" in January 2013.

Hervé Marchand   is Associate Editor of the IEEE Transactions on Automatic Control since 2009 and member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. He is member of the steering committee of MSR (Modélisation de systèmes réactifs). He was PC member of WODES'12, ICINCO'12. He is organizer of MSR 2013 in Rennes.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Nathalie Bertrand

Master : Techniques de vérification avancées, 10h, niveau M2, ISTIC, Université de Rennes 1.

Agrégation : Langages formels, 16h, niveau M2, ENS-Cachan-Antenne de Bretagne.

Sébastien Chédor

Licence : Programmation Java, 20h, niveau L2, ISTIC, Université de Rennes 1.
APF, 20h, niveau L1, ISTIC, Université de Rennes 1.
Initiation LaTeX, 6h, niveau L3, ENS-Cachan-Antenne de Bretagne.
Programmation, 20h, niveau L3, ENS-Cachan-Antenne de Bretagne.

Paulin Fournier

Licence : Scheme (TP), 20h, niveau L1, INSA-Rennes.

Christophe Morvan

Licence : Object Oriented programming with Java, 120h, niveau L2, Université de Marne-la-Vallée.
Systèmes d'exploitation (Cours), 36h, niveau L3, Université de Marne-la-Vallée.
Compilation (Cours-TD), 60h, niveau L3, Université de Marne-la-Vallée.

Amélie Stainer

Licence : Base de données (Cours-TD-TP), 28h, niveau L2, INSA-Rennes.

Agrégation : Modélisation (Cours), 11h, niveau M2, ENS-Cachan-Antenne de Bretagne.
Oraux blancs, 12h, niveau M2, ENS-Cachan-Antenne de Bretagne.
Préparation de leçons d'informatique, 10h, niveau M2, ENS-Cachan-Antenne de Bretagne.

8.2.2. Supervision

PhD in progress: **Sébastien Chédor**, Verification and test of systems modeled by regular graphs, started in September 2009, supervised by Christophe Morvan and Thierry Jéron.

PhD in progress: **Paulin Fournier**, Parameterized Verification of probabilistic systems, started in September 2012, supervised by Nathalie Bertrand and Thierry Jéron.

PhD in progress: **Srinivas Pinisetty**, Runtime validation of critical control-command systems, started in December 2011, supervised by Hervé Marchand and Thierry Jéron.

PhD in progress: **Amélie Stainer**, Quantitative verification of timed automata, started in October 2010, supervised by Nathalie Bertrand and Thierry Jéron.

8.2.3. Juries

Nathalie Bertrand was a member of the PhD defense jury of Youssouf Oualhadj (LaBRI, Bordeaux) in december 2012.

8.3. Popularization

Christophe Morvan has been involved in the organization of a public talk on Turing (celebrating the centenary of his birth) by Jean Lassègue. See the webpage.

ABSTRACTION Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Academy Members, Professional Societies

Patrick Cousot is a member of the Academia Europaea.

Patrick Cousot is member of the IFIP working group WG 2.3 on programming methodology.

Patrick Cousot is a member of the Board of Trustees and of the Scientific Advisory Board of the IMDEA-Software (Instituto madrileño de estudios avanzados—Research Institute in Software Development Technology), Madrid, Spain and of the Asian Association for Foundations of Software (AAFS).

9.1.2. Collective Responsibilities

Patrick Cousot is director of studies in computer science at ENS and member of the *commission de spécialistes* (hiring committee) of ENS.

Patrick Cousot, Antoine Miné and Xavier Rival are members of the lab council of the Laboratoire d'Informatique de l'École normale supérieure.

Jérôme Feret was a member of the *comité de sélection* (hiring committee) to hire an assistant professor at the Université de Lille 1.

9.1.3. Editorial Boards and Program Committees

— Patrick Cousot is member of the advisory board of the Higher-Order Symbolic Computation journal (HOSC, Springer) and of the Journal of Computing Science and Engineering (JCSE, Kiise).

Patrick Cousot is member of the steering committees of the Static Analysis Symposium (SAS) and the Verification, Model-Checking and Abstract Interpretation (VMCAI) international conference.

Patrick Cousot was member of the program committees of the Verified Software: Theories, Tools and Experiments (VSTTE 2012), Philadelphia, USA, January 28-29, 2012; Hybrid Systems: Computation and Control (HSCC 2012), Beijing, China, April 17-19, 2012; the Programming Languages day 2012, IBM Thomas J. Watson Center, New York, USA, June 29, 2012; the 19th Static Analysis Symposium (SAS 2012), Deauville, France, September 11-13, 2012; Hybrid Systems: Computation and Control (HSCC 2013), Philadelphia, PA, USA, April 9-11, 2013.

Patrick Cousot was the co-program committee chair of the Workshop on Systems Biology and Formals Methods (SBFM 2012), New York, NY, USA, March 29-30, 2012.

— Radhia Cousot is member of the advisory board of the Higher-Order Symbolic Computation journal (HOSC, Springer) and the Central European Journal of Computer Science (CEJCS, Versita & Springer).

Radhia Cousot is member of the steering committees of the Static Analysis Symposium (SAS), the Workshop on Numerical and Symbolic Abstract Domains (NSAD), the Workshop on Static Analysis and Systems Biology (SASB) and the Workshop on Tools for Automatic Program AnalysiS (TAPAS).

Radhia Cousot is the program committee chair of the 40th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL 2013), Rome, Italy, January 23-25, 2013.

Radhia Cousot was member of the program committee of the 13th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2012), January 22-24, 2012, Philadelphia, USA and Radhia Cousot is a member of the 5th NASA Formal Methods Symposium (NFM 2013), May 13-16, 2013, NASA Ames Research Center, California, USA.

— Jérôme Feret is a member of the editorial board of the Frontiers in Genetics journal.

Jérôme Feret is a member of the steering committee of the Workshop on Static Analysis and Systems Biology (SASB).

Jérôme Feret was co-program committee chair of the 3rd International Workshop on Static Analysis and Systems Biology (SASB 2012), Deauville, France, September 10, 2012; and of the Workshop on Systems Biology and Formals Methods (SBFM 2012), New York, NY, USA, March 29-30, 2012 and Jérôme Feret is co-program committee chair of the 4th International Workshop on Static Analysis and Systems Biology (SASB 2013), Seattle, WA, USA, June 2013.

Jérôme Feret was member of the program committees of the 4th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2012), St Maarten, Netherlands Antilles, March 25-30, 2012; the 2nd International Workshop on Interactions between Computer Science and Biology (CS2Bio 2012), Stockholm, Sweden, June 16, 2012; the International Symposium on Foundations of Health Information Engineering and System (FHIES 2012), Paris, France, August 27-28, 2012; the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013. Jérôme Feret is member of the program committee of the 5th International Conference on Bioinformatics, Biocomputational Systems and Biotechnologies (BIOTECHNO 2013), Lisbon, Portugal, March 24-29, 2013; the 4th International Workshop on Computational Models for Cell Processes (CompMod 2013), Turku, Finland, June 11, 2013.

— Jonathan Hayman was a member of the program committees of the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013.

— Antoine Miné is a member of the editorial boards of The Scientific World Journal in Computer Science and the Conference Papers in Computer Science journal.

Antoine Miné was co-chair of the program committee of the 19th International Static Analysis Symposium (SAS 2012), Deauville, France, 11–13 September 2012, and local organizer of SAS 2012 and affiliated events NSAD 2012, SASB'12 2012, TAPAS 2012, Deauville, France, 10–14 September 2012.

Antoine Miné was a member of the program committee of the Second International Workshop on Safety and Security in Cyber-Physical Systems (SSCPS 2012); Washington, DC, USA, 20–22 June 2012. Antoine Miné is a member of the program committee of the 20th International Static Analysis Symposium (SAS 2013), Seattle, WA, USA, 20–22 June 2013.

— Xavier Rival is member of the steering committee of the Workshop on Tools for Automatic Program AnalysiS (TAPAS).

Xavier Rival was member of the program committee of the program committee the European Symposium On Programming (ESOP 2012), Tallinn, Estonia, March 24 - April 1, 2012; the 40th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2013 ERC), Rome, Italy, January 23-25, 2013; the program committee of the program committee the European Symposium On Programming (ESOP 2013), Rome, Italy, March 2013.

9.1.4. Participation in Conferences

POPL: 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, Philadelphia, USA, January 25–27, 2012.
Patick Cousot attended the symposium and gave a talk on an abstract interpretation framework for termination [17].

Dagstuhl workshop: Dagstuhl Seminar 12051 Analysis of Executables: Benefits and Challenges, Dagstuhl, Germany, January 29–February 3rd, 2012.
Xavier Rival attended the workshop and gave a talk on the verification of programs manipulating complex data-structures.

TSD: 2th Tsingshua Software Day (Tsinghua University, Beijing, China, March 15, 2012).
Patrick Cousot gave a talk on automatic large-scale software verification by abstract interpretation.

SBFM: Workshop on Systems Biology and Formals Methods (New York, NY, USA, March 29-30, 2012).
Patrick Cousot, Jérôme Feret, and Norman Ferns attended to the workshop. Patrick Cousot and Jérôme Feret co-chaired the workshop. Patrick Cousot gave a talk called "A Causual Introduction to Abstract Interpretation" and Jérôme Feret gave a talk on model reduction of differential systems. Patrick Cousot and Jérôme Feret chaired some sessions.

ESOP: European Symposium on Programming (Tallinn, Estonia, March 24 – April 1, 2012)
Xavier Rival attended the conference. Xavier Rival chaired a session.

Bellairs Workshop: Workshop on Theory of Markov Processes (Bellairs Research Institute, Holetown, Barbados, April 2-6, 2012).
Jérôme Feret and Norman Ferns attended to the workshop. Jérôme Feret gave a talk on model reduction of stochastic semantics. Norman Ferns gave a talk on bisimulation metrics for continuous Markov decision processes.

NFM: 4th NASA Formal Methods Symposium (Norfolk, Virginia, April 3-5, 2012).
Patrick Cousot gave a talk on formal verification by abstract interpretation [12].

JCOMP: *Cinquièmes rencontres de la communauté française de compilation* (Rennes, France, 18–20 June 2012).
Antoine Miné attended the workshop and gave a talk.

WING: Fourth International Workshop on Invariant Generation (Manchester, UK, 30 June 2012).
Antoine Miné attended the workshop and gave an invited talk.

FMSB: Workshop on Formal Methods in Systems Biology (Berkeley, USA, July 7-8, 2012).
Jérôme Feret gave a talk on the model reduction of differential systems.

Dagstuhl workshop: Information Flow and Its Applications (Schloss Dagstuhl, Dagstuhl, Germany, August 26-31, 2012).
Jérôme Feret and Jonathan Hayman attended to the workshop. Jérôme Feret gave a talk on model reduction of differential semantics. Jonathan Hayman gave a talk on the semantics of Kappa and causal compression. Jérôme Feret chaired a session.

NSAD: Fourth International Workshop on Numerical and Symbolic Abstract Domains (Deauville, France, September 10, 2012).
Mehdi Bouaziz, Tie Cheng, David Delmas, Antoine Miné, Xavier Rival, Antoine Toubhans, and Caterina Urban attended the workshop. Xavier Rival chaired a session. Mehdi Bouaziz and Antoine Miné gave a talk [14], [23].

SASB: Third International Workshop on Static Analysis and Systems Biology (Deauville, France, September 10, 2012).
Ferdinanda Camporesi, Jérôme Feret, Norman Ferns, and Jonathan Hayman attended to the workshop. Jérôme Feret co-chaired the workshop and chaired half of the sessions.

SAS: 19th International Static Analysis Symposium (Deauville, France, September 11-13, 2012).
Mehdi Bouaziz, Ferdinanda Camporesi, Tie Cheng, David Delmas, Jérôme Feret, Norman Ferns, Jonathan Hayman, Vincent Laviron, Antoine Miné, Xavier Rival, Caterina Urban, and Antoine Toubhans attended the conference. Antoine Miné co-chaired the conference and chaired two sessions. Tie Cheng gave a talk [16].

TAPAS: Third International Workshop on Tools for Automatic Program Analysis (Deauville, France, Italy, France, September 14, 2012).
Ferdinanda Camporesi, Tie Cheng, David Delmas, Jérôme Feret, Norman Ferns, Jonathan Hayman, Antoine Miné, Xavier Rival, Antoine Toubhans, and Caterina Urban attended the workshop.

Dagstuhl workshop: Coalgebraic Information Flow and Its Applications, Schloss Dagstuhl, Dagstuhl, Germany, October 7-12, 2012.
Norman Ferns attended the workshop.

SBE: Systems Biology Europe, Madrid, Spain, October 16-17, 2012.
Jérôme Feret gave a talk on the model reduction of differential systems.

Workshop MSR   Workshop on "MSR-Inria joint centre", Cambridge (UK), November 5–6, 2012.
Xavier Rival attended the workshop and chaired a session. Xavier Rival gave a demo of ASTRÉE.

Workshop lif   Workshop "Let's imagine the future", Rennes (France), November 7–8, 2012.
Xavier Rival attended the workshop and gave a talk on the verification of embedded programs manipulating complex data-structures.

MOVEP: 10th school of Modelling and Verifying Parallel Processes (Marseille, France, 3–7 Dec. 2012).
Antoine Miné attended the school and gave a talk [24].

APLAS: 10th Asian Symposium on Programming Languages and Systems (Kyoto, Japan, 11–13 Dec. 2012).
Mehdi Bouaziz and Xavier Rival attended to the conference. Mehdi Bouaziz and Xavier Rival gave a talk [15], [26].

FSTTCS: IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, Hyderabad, India, December 15-17, 2012.
Jonathan Hayman attended the conference and gave a talk [20].

9.1.5. Invitations and Participation in Seminars

— Patrick Cousot gave an invited talk at the Computer Science PhD Day, Aula Magna Silvio Trentin, Universitá Ca' Foscari di Venezia, Italy, March 12th, 2012, and a distinguished lecture at the School of Computer Science of Carnegie Mellon University, Pittsburgh, PA, USA, April 12, 2012.

— Jérôme Feret gave some talks on model reduction for signaling pathways at the IMDEA-Softaware (Madrid, Spain) on the 15th of October, 2012, and at the Working Group of the Symbiose team-project (Rennes, France) on the 15th of November, 2012.

— Jonathan Hayman gave a talk at the Working Group on Computational Biology of the École normale supérieure (Paris, France) on the 28th of February, 2012, a talk at the Working Group of CEA List (Saclay, France) on 10th of April, 2012, and a talk at the seminar of the PPS team (Paris, France) on the 14th of June, 2012, about the semantics of Kappa and its causal compression.

— Xavier Rival gave a talk on "MemCAD, A Modular Abstract Domain for Reasoning on Memory States" at Microsoft Research (Redmond, USA) on the 23rd of July, 2012. Xavier Rival gave a talk on "Abstract domains for shape analysis" at CEA, on the 18th of February, 2012. Xavier Rival gave a talk on "MemCAD, a Modular Abstract domain for Reasoning about Memory States", at the Technical University of Vienna (TUW) on the 4th of September 2012.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence :

- Jérôme Feret, Mathematics, 40h ETD, L1, Licence Frontiers in Life Sciences (FdV), Université Paris-Descartes, France.

- Xavier Rival, Introduction to algorithmics, 40h ETD, L3, École Polytechnique, Palaiseau, France.

- Xavier Rival, Introduction to software verification, 12h ETD, L3, École Nationale Supérieure des Mines, Paris, France.

Master :

- Computational Biology, 9h ETD, M1. Interdisciplinary Approaches to Life Science (AIV), Master Program, Université Paris-Descartes, France.

- Patrick Cousot, Radhia Cousot, Jérôme Feret, Antoine Miné, and Xavier Rival, Abstract Interpretation: application to verification and static analysis, 72h ETD, M2. Parisian Master of Research in Computer Science (MPRI). École normale supérieure. France.
- Xavier Rival, 20h ETD, M1, École Polytechnique, Palaiseau, France.

9.2.2. *Supervision*

PhD & HdR :

PhD: Mattéo Zanioli, Security Analysis by Abstract Interpretation [8], March 2012, Radhia Cousot (co-directed thesis with Agostino Cortesi, University of Venice), Paris VII / Università Ca' Foscari, March 12, 2012.

PhD in progress:

- Mehdi Bouaziz, Static analysis of security properties by abstract interpretation. November 2011, Patrick Cousot, École Normale Supérieure.
- Ferdinanda Camporesi, Abstraction of Quantitative Semantics of Rule-based models, January 2009, Radhia Cousot and Jérôme Feret (co-directed thesis with Maurizio Gabrielli, University of Bologna).
- Tie Cheng, Static analysis of spreadsheet macros, October 2011, Xavier Rival, École Polytechnique
- Vincent Laviron, Static Analysis of Functional Programs by Abstract Interpretation, October 2009, Patrick Cousot, École Normale Supérieure.
- Antoine Toubhans, Combination of shape abstract domains, October 2011, Xavier Rival, École Doctorale de Paris Centre
- Caterina Urban, Static Analysis of Functional Temporal Properties of Programs by Abstract Interpretation, November 2011, Radhia Cousot, École Normale Supérieure.

9.2.3. *Juries*

— Jérôme Feret reviewed the PhD thesis of Vincent Noël (Université Rennes 1, France, December 20, 2012).

— Xavier Rival reviewed the PhD theses of Arnaud Jobin (IRISA, Rennes, France, January 16, 2012), of Marie Pelleau (LINA, Nantes, France, November 29, 2012) and of Arnault Ioualalen (DALI /UPVD, Perpignan, France, December 17, 2012).

9.3. Popularization

— Xavier Rival gave a talk at the "1/2 heure de Science", at Inria Rocquencourt, on the 6th of December, 2012.

ATEAMS Project-Team

7. Dissemination

7.1. Scientific Animation

7.1.1. Teaching

Master : Jurgen Vinju, Paul Klint, Software Evolution, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Tijs van der Storm, Jurgen Vinju, Software Construction, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Jan van Eijck, Bert Lisser, Software Testing, 6 EC, Universiteit van Amsterdam, The Netherlands

Master : Paul Klint, EASY Meta-Programming with Rascal, full-day course at Summer School on Language Frameworks, Sinaia, Romania

Master : Paul Klint, Rascal tutorial, one-day course, FUNDP, Namur, Belgium

Master : Tijs van der Storm, one-day course on Rascal, Universidade do Minho (Braga)

Graduate: Tijs van der Storm, one-day course on Rascal, Programming Language class, UT Austin, U.S.A.

7.1.2. Supervision

PhD : Floor Sietsma, Logics of Communication and Knowledge, Universiteit van Amsterdam, 13-12-2012, supervisors Jan van Eijck, Krzysztof Apt

PhD in progress : Paul Griffioen, Next Generation Computational Auditing, started 2011, supervisors Paul Klint, Philip Elsas

PhD in progress : Anastasia Izmaylova, A General Language Parametric Framework for Software Refactoring, started 2011, supervisors Paul Klint, Jurgen Vinju

PhD in progress : Jeroen van den Bos, Digital Forensics Software Engineering, started 2010, supervisors Paul Klint, Tijs van der Storm

PhD in progress : Atze van der Ploeg, Rapid Language Parametric Prototyping of Software Visualization and Exploration, started 2011, supervisor Paul Klint.

PhD in progress : Davy Landman, Recovery and Synthesis of Domain Specific Language Design, started 2011, supervisors Jurgen Vinju, Paul Klint, supervisors Jurgen Vinju, Paul Klintto .

PhD in progress : Riemer van Rozen, Software Engineering Principles for the Gaming Domain, started 2011, supervisor Paul Klint

PhD in progress : Ali Afroozeh, Ambiguity and Disambiguation for Context-free Grammars, started 2012, supervisor Jurgen Vinju

PhD in progress : Ashim Shahi, Principled Quality Assessment of Software, started 2012, supervisor Paul Klint, Jurgen Vinju

PhD in progress : Michael Steindorfer, Scaling meta-programming to data-programming, started 2012, supervisor Paul Klint, Jurgen Vinju

Paul Klint, Jurgen Vinju, Tijs van der Storm and Jan van Eijck together also supervised more than 30 master thesis projects for Universiteit van Amsterdam in 2012.

7.1.3. Juries

- Jurgen Vinju, PhD: Veronica Isabel Uquillas Gomez, Vrije Universiteit Brussel & Université Lille, Belgium & France.
- Paul Klint, PhD: J. Dormans, Universiteit van Amsterdam, The Netherlands.
- Paul Klint, PhD: R. Poss, Universiteit van Amsterdam, The Netherlands.
- Paul Klint, PhD: L. Kwiatkowski, Vrije Universiteit, The Netherlands.
- Jan van Eijck, PhD: Peter Gammie, University of Camberra, Australia.

7.1.4. Invited speakers

- Jurgen Vinju - IFIP WG 2.4, Vadstena, Sweden.
- Tijs van der Storm - IFIP TC2 2.16, London, England.
- Tijs van der Storm - IFIP TC2 2.16, Austin, U.S.A.
- Paul Klint - Invited speaker at PReCISE Conference, Namur, Belgium.
- Paul Klint - Keynote "The Spinoff Game" at Entrepreneurial Research Day, ICT Labs, Paris, France.
- Mark Hills - Invited speaker at International Workshop On Rewriting Logic and its Applications, Talinn, Estonia.

7.1.5. Positions, memberships and editorial work

- Jan van Eijck : Member of the European Network in Computational Logic
- Jan van Eijck : Member of the International Quality Assessment Committee
- Jan van Eijck: Member of the NWO committee "Vrije Competitie" for Computer Science.
- Jan van Eijck: Book editor "Games, Actions, and Social Software", Springer.
- Jan van Eijck: Program committee IWCS
- Jan van Eijck: Program committee LORI-4
- Jan van Eijck: Reviewer ESSLLI
- Jan van Eijck: Reviewer Journal of Semantics
- Jan van Eijck: Reviewer Journal of Logic and Computation
- Jan van Eijck: Reviewer Fundamenta Informaticae
- Jan van Eijck: Reviewer Synthese
- Jan van Eijck: Reviewer Journal of Philosophical Logic
- Jan van Eijck: Reviewer Journal of Logic, Language and Information
- Jan van Eijck: Cambridge University Press, Australian National University (Canberra)
- Tijs van der Storm: Program co-chair IPA Lentedagen
- Tijs van der Storm: External reviewer OOPSLA
- Tijs van der Storm: External reviewer POPL 2013
- Tijs van der Storm: Reviewer Information and Software Technology
- Tijs van der Storm: Reviewer Software Practice & Experience
- Tijs van der Storm: Science of Computer Programming
- Mark Hills : Reviewing Software Practise & Experience
- Mark Hills : Reviewing IET Software
- Mark Hills : Program committee FMOODS
- Paul Klint : Editor for Science of Computer Programming
- Paul Klint : Editor for Springer Service Science Book Series

- Paul Klint : Visiting Professor University of London, Royal Holloway
- Paul Klint : Treasurer European Association for Programming Languages and Systems (EAPLS)
- Paul Klint : Steering committee member ETAPS
- Paul Klint : Board member Instituut voor Programmatuur en Architectuur (IPA)
- Paul Klint : External advisor PlanComps project (UK)
- Paul Klint : Full Professor at UvA, Software Engineering Chair
- Paul Klint : Director Master Software Engineering, UvA
- Paul Klint : Treasurer European Association for Programming Languages and Systems (EAPLS)
- Paul Klint : Steering committee member ETAPS
- Paul Klint : Board member Instituut voor Programmatuur en Architectuur (IPA)
- Paul Klint : Program committee SLE
- Jurgen Vinju : Head of CWI Research group Software Analysis and Transformation (SEN1)
- Jurgen Vinju : Program committee ICMT
- Jurgen Vinju : Program committee CC
- Jurgen Vinju : Program committee SCAM
- Jurgen Vinju : Steering committee SCAM
- Jurgen Vinju : Steering committee SLE
- Jurgen Vinju : Co-organizer workshop SL(E)BOKSLE
- Jurgen Vinju : Member Working Council (CWI)
- Jurgen Vinju : Workshop selection chair SLE
- Jurgen Vinju : Reviewing Journal of Software Maintenance and Evolution: Research and Practice
- Jurgen Vinju : Reviewing Transactions on Software Engineering (TSE)
- Jurgen Vinju : Reviewer Journal on Empirical Software Engineering (EMSE)
- Jurgen Vinju : Reviewer Science of Computer Programming (SCP)
- Jurgen Vinju : Member meetings between Inria & CWI management, Paris and Amsterdam.
- Vadim Zaytsev: Program committee LDTA
- Vadim Zaytsev: Program committee SCAM
- Vadim Zaytsev: Program committee SQM
- Vadim Zaytsev: Program committee Wikimedia Conference Netherlands
- Vadim Zaytsev: Reviewer Science of Computer Programming (SCP)
- Vadim Zaytsev: Reviewer Journal on Empirical Software Engineering (EMSE)
- Vadim Zaytsev: Reviewer IET Software
- Vadim Zaytsev: Program chair Wikimedia Conference Netherlands (WCN)
- Vadim Zaytsev: Social media chair SoTeSoLa
- Vadim Zaytsev: Hackathon coordinator SoTeSoLa
- Vadim Zaytsev: Colloquium organiser of Programming Environment Meetings (PEM)

7.2. Popularization

In 2012 our team has invested a large amount of time and energy in reaching out, in close collaboration with our support staff:

- The "Understanding Software" symposium with more than 250 participants from industry and academia. This was organized in honor of celibrating the 40th anniversary of Paul Klint at CWI. The symposium was a great success, with internationally renowned speakers and a large and diverse audience. The topic was entirely devoted to the research topics of our team.

- Turing centennial exposition, including Enigma machine and X1, hosted more than 1000 visitors.

- Lego Turing Machine, including IDE, was an online hit with millions of viewers. Articles about the machine and its meaning appeared in all major Dutch journals and we estimate a reach of more than 3 million readers.

- ICT Delta - we presented at the Dutch national symposium ICT Delta where industry meets academia in ICT.

- Floor Sietsma appeared on national television and radio, and in most newspapers to explain about her role as the youngest Phd candidate and her research.

- Paul Klint chaired public discussion on Government Data Policy, IPoort, The Hague, April 10, 2012

- Jurgen Vinju went to different companies to explain about Rascal and building your own software metrics, and software engineering in general (Sogyo, Software Factory)

- Tijs van der Storm, Jurgen Vinju and Vadim Zaytsev presented at "IPA Spring Days" about domain specific languages and related topics to all Dutch PhD students in Computer Science.

- Tijs van der Storm organized a Lisp course for Devnology

- Tijs van der Storm presented at Optiver about Domain-Specific Languages

CARTE Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Responsibilities

Guillaume Bonfante:

- was a member of the program committee of the workshop DICE 2012, Tallinn, Estonia,
- refereed some projects for the Netherlands Organisation for Scientific Research (NWO).

Isabelle Gnaedig is:

- co-leader of the EPI Carte,
- member of the scientific mediation committee of Inria Nancy Grand-Est,
- member of the engineer recruitment committee of Inria Nancy-Grand Est,
- social referee at Inria Nancy-Grand Est.

Mathieu Hoyrup is:

- the organizer of the Seminar of the LORIA Department "Formal Methods".

Jean-Yves Marion is:

- head of the EPI Carte,
- head of the High Security Lab,
- member of the executive committee of Inria Nancy-Grand Est,
- member if the AERES visiting committee,
- member of the CNU, section 27,
- member of the steering committee of DICE and LCC,
- chair of Malware 2012 and PC member of PREW 2012,
- co-organizer of a winter school at CIRM (one week on complexity).

Romain Pechoux is:

- principal investigator of the Inria associate team Cristal.

9.1.2. Talks

Guillaume Bonfante:

- talk at the "Rewriting and Logic Seminar" at the JAIST (Japan Advanced Institute of Science and Technology), Kanazawa, March 2012.

Emmanuel Hainry:

- presentation at Logic and Interactions 2012, complexity week in Marseille, January 30th to February 3rd, 2012.

Mathieu Hoyrup:

- invited to give the talk "On the inversion of computable functions" at the 7th International Conference on Computability, Complexity and Randomness, in Cambridge, July 2012,
- gave the talk "Computability in Ergodic Theory" at the Journées Calculabilités, Paris, March 5 and 6, 2012.

Emmanuel Jeandel

- invited to give a four hours minicourse: "Computational aspects of multidimensional symbolic dynamics", at the first DySyCo school (Dynamical Systems and Computation) in Santiago, Chile, December 2012.

Jean-Yves Marion

- talk on computer viruses at Corte, September, 2012 and at Grenoble, December, 2012,
- two talks on computer viruses at Bloomington, Indiana University, October 29th and October 31st, 2012.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence:

- Guillaume Bonfante:
  - Java, L3, Ecole des Mines, Université de Lorraine, France.
- Emmanuel Hainry:
  - Operating Systems, 60 h, L1, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Algorithms and Programs, 60 h, L1, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Object Oriented Programming, 24 h, L1, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Databases, 24 h, L2, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Advanced Databases, 20 h, L2, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Complexity, 28 h, L2, IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Algorithmics, 12 h, DU PFST (equiv. L1), IUT Nancy Brabois, Université de Lorraine, Nancy, France,
  - Operating Systems, 9 h, DU PFST (equiv. L1), IUT Nancy Brabois, Université de Lorraine, Nancy, France.
- Emmanuel Jeandel
  - Probability for Computer Science, 46 hours, L3 Informatique, FST, Université de Lorraine, Nancy, France.
- Romain Péchoux:
  - c2i, 20, L1 , Université de Lorraine, Nancy, France,
  - Propositional logic, 25 hours, L1 ISC, UFR MI, Université de Lorraine, Nancy, France,
  - Introduction to Java, 45 hours, L3 ISC MIAGE , UFR MI, Université de Lorraine, Nancy, France,
  - Databases, 42 hours, L3 LSG, ISAM-IAE, Université de Lorraine, Nancy, France,
  - Algorithmic complexity, 30 hours, L3 ISC MIAGE, IGA, Casablanca, Maroc.

Master:

- Guillaume Bonfante:

- – Modelling and UML, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
        - – Video games, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
        - – Semantics, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
        - – Safety of software, M2, Ecole des Mines, Université de Lorraine, Nancy, France.
- Isabelle Gnaedig:
    - – "Design of Safe Software", Coordination of the module, M2, ESIA-Telecom (Université de Lorraine), Nancy, France,
    - – "Rule-based Programming", 20 hours, M2, ESIAL-Telecom (Université de Lorraine), Nancy, France.
- Emmanuel Jeandel:
    - – Algorithms and Complexity, 35 hours, M1 Informatique, FST, Université de Lorraine, Nancy, France.
- Jean-Yves Marion:
    - – Automata Theory, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
    - – Logic, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
    - – Data Base, M1, Ecole des Mines, Université de Lorraine, Nancy, France,
    - – Algorithmic, M1, Ecole des Mines, Université de Lorrain, Nancy, France,
    - – Security, M2, Ecole des Mines, Université de Lorraine, Nancy, France,
    - – Head of the M2 internships, M2, Ecole des Mines, Université de Lorraine, Nancy, France.
- Romain Péchoux:
    - – Advanced Java, 52 hours, M1 MIAGE, UFR MI, Université de Lorraine, Nancy, France,
    - – Mathematics for computer science, 20 hours, M1 SCA, UFR MI, Université de Lorraine, Nancy, France.

9.2.2. Supervision

PhD : Pascal Vanier, "Pavages : périodicité et complexité calculatoire", Aix-Marseille Université, defended November 22th, 2012, Emmanuel Jeandel.

PhD in progress : Thanh Dinh Ta, Malware Algebraic Modeling and Detection, started Sept. 2010, Jean-Yves Marion (director) and Romain Péchoux (co-advisor).

PhD in progress: Hugo Férée, Computational Complexity in Analysis, started Sept. 2011, Jean-Yves Marion (director) and Mathieu Hoyrup (co-advisor).

PhD in progress: Aurélien Thierry, Morphological Analysis of Malware, started October 2011, Jean-Yves Marion.

PhD in progress: Joan Calvet, Viruses: how they interact with their environment, started October 2009, Jean-Yves Marion and José M. Fernandez, joint PhD with Ecole Polytechnique de Montréal.

9.2.3. Juries

Isabelle Gnaedig:

- participation to the ESIAL-Telecom admission committee.

Emmanuel Hainry:

- in charge of the admission committee for dept. Réseaux et Télécoms at IUT Nancy Brabois.

Mathieu Hoyrup:

- participation to the jury of Master 2 "Logique Mathématique et Fondements de l'Informatique" of Benoît Monin.

Jean-Yves Marion:

- November 30th, 2012, HDR of Virgile Mogbil, U. Paris 13 (reviewer),
- December 3th, 2012, PhD of Vincent Cheval, ENS Cachan (president),
- December 6th, 2012, PhD of Antoine Madet (reviewer),
- December 7th, 2012, PhD of Vincent Demange,
- December 13th, 2012, HDR of Emmanuel Thomé,
- December 17th, 2012, PhD of Hedi Benzina, ENS Cachan (reviewer).

Romain Péchoux:

- participation to the UFR MI, licence Miage, admission committee.

9.3. Popularization

Guillaume Bonfante:

- talk at the "Rendez-Vous du Numérique et de l'Intelligence Economique", about "Computer viruses", Strasbourg, October 2012,
- talk at the "Journées francophones de l'investigation numérique (JFIN)", about "Les virus, amis ou ennemis de l'investigation numérique ? ", Levallois-Perret, November 2012.

Emmanuel Hainry:

- presentation at Inria Jam Session 2012, June 19th, 2012 http://www.inria.fr/centre/nancy/agenda/jam-session-alumni.

Jean-Yves Marion:

- redaction of an article in "Pour la Science" http://www.pourlascience.fr/ewb_pages/f/fiche-article-les-i-mac-i-resistent-ils-mieux-aux-virus-que-les-i-pc-i-30414.php.

CASSIS Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorial board

- Information & Computation (Véronique Cortier)
- Journal of Computer Security (Véronique Cortier)

9.1.2. Conferences

- FroCoS 2013, 9th Symposium on Frontiers of Combining Systems, 18–20 September 2013, Nancy, France, (Christophe Ringeissen, conference chair)

9.1.3. Program committees

- Fabrice Bouquet: MODEVVA 2012, ICST 2013 (Publicity Chair)
- Véronique Cortier: CSF 2012 (co-chair), CCS 2012, ESORICS 2012, POST 2012, FCC 2012, SCSS 2012, LPAR 2012, MOVEP 2012.
- Frédéric Dadeau: CSTVA 2012 (co-chair)
- Alain Giorgetti: TAP 2012
- Pierre-Cyrille Héam: IHTIAP 2012
- Abdessamad Imine: DEXA 2012, CIIA 2013
- Steve Kremer: ACNS 2012, CSF 2012, FSTTCS 2012, ISPEC 2012, POST 2012, TGC 2012
- Christophe Ringeissen: CADE-24, FroCoS 2013
- Michaël Rusinowitch: CRISIS 2012, GRSRD 2012 (co-chair), IJCAR 2012, QASA 2012, SCSS 2012, WooPS12

9.1.4. Summer school

- TAROT 2012, 8th International Summer School on Training And Research On Testing, 2–6 July 2012, Métabief, France, (Frédéric Dadeau, general chair)

9.1.5. Working groups

- GT-Verif, Verification, GDR IM Working Group (Véronique Cortier, chair)
- MTV2, Testing Methods for Verification and Validation, GDR GPL Working Group (Frédéric Dadeau, co-chair)
- FORWAL, Formalisms and Tools for Verification and Validation, GDR GPL Working Group (Pierre-Cyrille Héam, co-chair)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence :

  Frédéric Dadeau, Algorithmics and Programming, 80 hours (ETD), L1, University of Franche-Comté, France

  Frédéric Dadeau, Databases, 40 hours (ETD), L1, University of Franche-Comté, France

  Frédéric Dadeau, Object-Oriented Modelling and Conception, 40 hours (ETD), L3, University of Franche-Comté, France

  Frédéric Dadeau, Web Languages, 26 hours (ETD), L2, University of Franche-Comté, France

  Alain Giorgetti, Logics and Deduction, 52 hours (ETD), L2, Université de Franche-Comté, France

  Alain Giorgetti, Formal Methods, 81 hours (ETD), L3, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Discrete Mathematics, 190 hours (ETD), L1/L2, IUT Belfort-Montbéliard, France

  Olga Kouchnarenko, Formal languages and automata, 95 hours (ETD), L3, University of Franche-Comté, France

  Olga Kouchnarenko, Syntactic analysis and XML, 33 hours (ETD), L3, University of Franche-Comté, France

- Master :

  Fabrice Bouquet, Compilation, 81 hours (ETD), M1, Université de Franche-Comté, France

  Fabrice Bouquet, Method et Tools For Artificial Intelligence, 40 hours (ETD), M1, Université de Franche-Comté, France

  Fabrice Bouquet, Test, 30 hours (ETD), M2, Université de Franche-Comté, France

  Véronique Cortier, Security Theory, 37 hours (ETD), M2, Lorraine University, France

  Frédéric Dadeau, Testing, 22 hours (ETD), M2, University of Franche-Comté, France

  Alain Giorgetti, Program Proofs, 60 hours (ETD), M1, Université de Franche-Comté, France

  Alain Giorgetti, Decision Procedures, 13 hours (ETD), M2, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Introduction to calculability, 22 hours (ETD), M2, Université de Franche-Comté, France

  Pierre-Cyrille Héam, Automata based Verification, 20 hours (ETD), M2, Université de Franche-Comté, France

  Abdessamad Imine, Security for XML Documents, 12 hours (ETD), M1, University of Lorraine, France

  Olga Kouchnarenko, Components and security, 12 hours (ETD), M2, University of Franche-Comté, France

  Olga Kouchnarenko, Specification, verification and validation, 15 hours (ETD), M2, University of Franche-Comté, France

  Olga Kouchnarenko, Modelling and evaluation of complex systems, 20 hours (ETD), M2, University of Franche-Comté, France

- Doctorat :

  Fabrice Bouquet, Model Based Testing for Functional and Security Test, 4 hours (ETD), 12th edition of the International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy

9.2.2. Supervision

- PhD :

Jonathan Lasalle, Génération automatique de tests à partir de modèles SysML pour la validation fonctionnelle de systèmes embarqués, Université de Franche Comté, June 29th, Fabrice Bouquet and Fabien Peureux

Elizabeta Fourneret, Génération de tests à partir de modèles UML/OCL pour les systèmes critiques évolutifs, Université de Franche Comté, December 5th, Fabrice Bouquet

Asma Chérif, Modèles de Contrôle d'Accès pour les Applications Collaboratives, Université de Lorraine, November 26th, Abdessamad Imine and Michaël Rusinowitch

- PhD in progress :

Kalou Cabrera Castillos, Automated Test Generation from Property Patterns, started in December 2009, Frédéric Dadeau and Jacques Julliand

Rémy Chrétien, Decision procedures of equivalence properties, started in October 2012, Véronique Cortier and Stéphanie Delaune

Aloïs Dreyfus, Efficient approches for systems validation, started in Novembre 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

Ivan Enderlin, Test Data Generation for Unit Testing in PHP, started in October 2011, Fabrice Bouquet, Frédéric Dadeau and Alain Giorgetti

Jean-Marie Gauthier, Method for validation and simulation of SysML model: Applied on microsystems, started in October 2012, Fabrice Bouquet, Fabien Peureux and Ahmed Hammad

Richard Genestier, Formal specification and verification of programs generating structured data, started in October 2012, Alain Giorgetti and Olga Kouchnarenko

Bao-Thien Hoang, Secure Collaboration in Social Networks, started in April 2011, Abdessamad Imine and Christophe Ringeissen

Vincent Hugot, Approximations and Constraints: Application to the Verification of Embedded Systems, started in October 2010, Pierre-Cyrille Héam and Olga Kouchnarenko

Jean-Luc Joly, Randomized approaches for validation and verification procedures, started in December 2011, Pierre-Cyrille Héam

Robert Künnemann, Verification of Security APIs, started in October 2010, Steve Kremer and Graham Steel

Houari Mahfoud, Access Control Models for XML Documents, started in September 2010, Abdessamad Imine and Michaël Rusinowitch

Guillaume Scerri, Symbolic and automatic security proofs in computational models, started in September 2011, Hubert Comon-Lundh and Véronique Cortier

Elena Tushkanova, Specification and formal certification of (combinations of) decision procedures, started in October 2009, Alain Giorgetti, Olga Kouchnarenko and Christophe Ringeissen

Cyrille Wiedling, Formal analysis of E-voting protocols, started in September 2011, Véronique Cortier

9.2.3. *Juries*

Inria evaluation committee (Véronique Cortier, Michaël Rusinowitch)

Referee for Karine Mordal's PhD, December 2012, Paris: Analyse et conception d'un modèle de qualité logiciel (Fabrice Bouquet)

Referee for Benoît Groz' PhD, October 2012, Lille: XML Security Views Queries, Updates, and Schema (Michaël Rusinowitch)

Referee for Marion Daubignard's PhD, January 2012, Grenoble: Formal Methods For Concrete Security Proofs (Steve Kremer)

Referee for Antoun Yaacoub's PhD, November 2012, Toulouse: Information Flow in Logic Programming (Olga Kouchnarenko)

Committee chair for Lionel Droz-Bartholet's PhD, February 2012, Besançon: Conception, validation et évaluation d'un nouveau protocole de gestion de la mémoire partagée collaborative tolérant aux pannes (Fabrice Bouquet)

Committee chair for Qianxue Wang's PhD, March 2012, Besancon, France: A new familly of chaotic pseudo-random generators (Pierre-Cyrille Héam)

Committee chair for Lamiel Toch's PhD, November 2012, Besancon, France: Contribution to scheduling techniques on parallel and ditributive systems (Pierre-Cyrille Héam)

Examiner for Muhammad Naeem Irfan's PhD, September 2012, Grenoble, France: Analysis and optimisation of machine learning algorithms for software components (Frédéric Dadeau)

9.3. Popularization

Invited conference of Véronique Cortier at the national annual days of the APMEP (Association des Professeurs de Mathématiques de l'Enseignement Public), Metz, October 27-30, 2012.

Invited conference of Fabrice Bouquet at Software Quality Club (association of software professional): "Model-based Testing today", Paris, January 24, 2012

Invited conference of Fabrice Bouquet at 6th SysML France conference: "Test generation from SysML Model", Mulhouse, November 13, 2012

Interview of Véronique Cortier for the Information Letter of Info CST Lorraine (Culture Scientifique et Technique), issue 87, January 2012.

Participation of Véronique Cortier in a documentary film on the life of Alan Turing (film director: Catherine Bernstein)

Participation of Véronique Cortier in the Big Data report, published at *CNRS Le Journal*, November 2012.

"Le vote électronique est-il anti-démocratique par essence ?" by Steve Kremer and Christophe Castro in Inriality, March 29, 2012.

Inria Alumni Jam Session organized by Steve Kremer, Nancy, June 19, 2012.

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

8. Dissemination

8.1. Scientific Animation

David Pichardie served on the program committees of the international conferences IFM 2012 and ITP 2012 and the international workshop SVARM & VERIFY 2012. He co-chaired the international workshop PxTP 2012. A. Schmitt is a member of the steering committee of the Journées Françaises des Langages Applicatifs (JFLA). Thomas Jensen and Alan Schmitt organized the École Jeunes Chercheurs en Programmation (EJCP 2012). Sandrine Blazy served on the organizing committee of the annual meeting of the GDR GPL French community. Sandrine Blazy is a member of the steering committe of the ITP conference. Sandrine Blazy is scientific director of the "Languages and software engineering department" of IRISA.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Alan Schmitt, Caml, 43h, L3, Insa Rennes, France

Alan Schmitt, Méthodes Formelles pour le développement de logiciels sûrs, 12h, M1, Rennes 1, France

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

Sandrine Blazy, Software vulnerabilities, 24h, M2PRO, Rennes 1

Sandrine Blazy, Mechanised semantics, 30h, M2R, Rennes 1, France

Sandrine Blazy, The Coq proof assistant, 6h, 4th Asian-Pacific summer school on formal methods, Shanghai, China

Sandrine Blazy, Functional programming, 30h, L3, Rennes 1, France

Frédéric Besson, Compilation, 30h, M1, Insa Rennes, France

Thomas Jensen, Program analysis and Semantics, 30h, M2R, Rennes 1, France

Thomas Jensen, Sécurité de logiciel, 30h, M2R, Rennes 1, France

Pierre-Alain Fouque, Cryptography, 58h, M2PRO, Rennes 1, France

Thomas Jensen, Static program analysis, 5h, Ecole Jeunes Chercheurs en Programmation.

Thomas Genet, Cryptography, 18h, M1, Rennes 1, France

Thomas Genet, Object-oriented software engineering, 48h, M1, Rennes 1, France

Thomas Genet, Software Formal Analysis and Design, 65h, M1, Rennes 1, France

Thomas Genet, Functional programming, 44h, L3, Rennes 1, France

David Cachera, Programming language semantics, 24h, M1, Rennes 1, France

David Cachera, Computability and Logic, 24h, L3, ENS Cachan Bretagne, France

David Cachera, Formal Languages, 24h, L3, ENS Cachan Bretagne, France

David Cachera, Algorithmics, 10h, M2FES, ENS Cachan Bretagne, France

8.2.2. Supervision

PhD & HdR :

HdR : David Pichardie, Toward a Verified Software Toolchain for Java, ENS Cachan, November 19th 2012

PhD : Delphine Demange, Semantic foundations of intermediate program representations, ENS Cachan, October 19th 2012, Thomas Jensen and David Pichardie

PhD : Arnaud Jobin, Dioïdes et idéaux de polynômes en analyse statique, ENS Cachan, January 16th 2012, Thomas Jensen and David Cachera

PhD in progress: Zhoulai Fu, Abstract interpretation and memory analysis, octobre 2009, Thomas Jensen and David Pichardie

PhD in progress: Vincent Laporte, Formal verification of static analyses for low level langages, septembre 2012, Sandrine Blazy and David Pichardie

PhD in progress: Martin Bodin, Certified Analyses for JavaScript, September 2012, Thomas Jensen and Alan Schmitt

PhD in progress: Andre Oliveira Maroneze, Compilation vérifiée et calcul de temps d'exécution au pire cas, septembre 2010, Sandrine Blazy and Isabelle Puaut

PhD in progress: Stéphanie Riaud, Transformations de programmes pertinentes pour la sécurité du logiciel, septembre 2011, Sandrine Blazy

PhD in progress: J-C Zapalowicz, Formal methods for identifying security vulnerabilities, September 2011, Thomas Jensen and Pierre-Alain Fouque.

Pierre-Emmanuel Cornilleau: Result certification of static analyses using SMTs, October 2009, Frédéric Besson and Thomas Jensen.

PhD in progress: Valérie Murat, Automatic verification of infinite state systems using tree automata completion, septembre 2010, Thomas Genet

PhD in progress: Yann Salmon, Static Analysis of functional programs using tree automata, septembre 2011, Thomas Genet

8.2.3. *Juries*

Alan Schmitt, jury member for the HdR defense of Ludovic Henrio, July 19th 2012

Alan Schmitt, jury member (reviewer) for the PhD defense of Federico Ulliana, December 12 2012

Sandrine Blazy, jury member for the HDR defense of Eric Totel, December 2012, Supélec, Rennes

Sandrine Blazy, jury member (reviewer) for the PhD defense of Vincent Filou, December 2012, LABRI, Bordeaux

Thomas Jensen, jury member (reviewer) for the PhD defense of Tahina Ramananandro, January 2012, ENS Paris

Thomas Jensen, jury member (examiner) for the PhD defense of Jérémy Planul, February 2012, Ecole polytechnique

Pierre-Alain Fouque, jury member (reviewer) for the PhD defense of Olivier Meynard, January 2012, ENST Paris

Pierre-Alain Fouque, jury member (reviewer) for the PhD defense of Sylvain Heraud, February 2012, Nice-Sophia Antipolis

Pierre-Alain Fouque, jury member (reviewer) for the PhD defense of Christina Boura, January 2012, Paris 6 University

8.3. Popularization

David Pichardie organised the second edition of the french Castor Informatique contest. This contest promotes Computer Science in secondary schools and high schools. It is organised by Inria, ENS Cachan and the France IOI association and supported by CNRS, Pascaline, the SIF and API associations. In 2012, there was about 90.000 participants.

Sandrine Blazy was interviewed for a 10 minutes podcast (in French) about compiler verification. The podcast is available from the Interstices website.

COMETE Project-Team

8. Dissemination

8.1. Animation of the scientific community

Note: In this section we include only the activities of the permanent internal members of Comète.

8.1.1. Editorial activity

Catuscia Palamidessi is:

Member of the Editorial Board of Mathematical Structures in Computer Science, published by the Cambridge University Press.

Member of the Editorial Board of the Electronic Notes of Theoretical Computer Science, Elsevier Science.

Co-editor (with Frank Pfenning) of the special issue of Logical Methods in Computer Science dedicated to selected papers of FoSSaCS 2013.

Co-editor (with Geoffrey Smith) of the special issue of Mathematical Structures in Computer Science dedicated to Quantitative Information Flow.

Co-editor (with Samson Abramsky and Michael Mislove) of the special issue of Theoretical Computer Science dedicated to selected papers of MFPS XXV. [33]

Co-editor (with Sebastian Mödersheim) of the proceedings of TOSCA 2011, Theory of Security and Applications. [34]

Co-editor (with Mark Ryan) of the proceedings of TGC 2012, Trustworthy Global Computing. [35]

Frank D. Valencia is:

Co-editor of the special issue of Mathematical Structures in Computer Science dedicated to the 18th International Workshop on Expressiveness in Concurrency.

Co-editor of the special issue of Mathematical Structures in Computer Science dedicated to the 17th International Workshop on Expressiveness in Concurrency.

Konstantinos Chatzikokolakis and Catuscia Palamidessi are:

Co-editors (with Sebastian Mödersheim) of the special issue of the Journal of Computer Security dedicated to selected papers of TOSCA 2011 and SecCo 2011.

8.1.2. Steering Committees

Catuscia Palamidessi is member of:

The Council of EATCS, the European Association for Theoretical Computer Science. Since 2005.

The Steering Committee of ETAPS, the European Joint Conferences on Theory and Practice of Software. Since 2006.

The IFIP Technical Committee 1 – Foundations of Computer Science. Since 2007.

The IFIP Working Group 2.2 – Formal Description of Programming Concepts. Since 2001.

The IFIP Working Group 1.7 – Theoretical Foundations of Security Analysis and Design. Since 2010.

Frank D. Valencia member of:

The steering committee of the International Workshop in Concurrency EXPRESS. Since 2010.

8.1.3. Invited Talks

Catuscia Palamidessi has given invited talks at the following conferences and workshops:

Grande Region Security and Reliability Day. Nancy, France. March 2012.

COW 2012. The 19th CREST Open Workshop on *Interference and Dependence* on 30st April - 1st May 2012.

VECoS 2012. 6th International Workshop on Verification and Evaluation of Computer and Communication Systems. CNAM, Paris, France. August 27-28, 2012.

8.1.4. Organization of workshops and conferences

Catuscia Palamidessi has served as PC co-chair (together with Mark Ryan) of TGC 2012, the 7th International Symposium on Trustworthy Global Computing. Newcastle, UK, 7-8 September 2012.

Catuscia Palamidessi has co-organized (together with Boris Köpf and Pasquale Malacaria) the Dagstuhl seminar on Quantitative Security Analysis. Dagstuhl, Germany, 25-30 November 2012.

8.1.5. Participation in program committees

Catuscia Palamidessi has been/is a member of the program committees of the following conferences:

TGC 2013. The 8th International Symposium on Trustworthy Global Computing. Buenos Aires, Argentina, 30-31 August 2013.

ICALP 2013 Track B. The 40th International Colloquium on Automata, Languages and Programming. Riga, Latvia, 8-12 July 2013.

CSF 2013. The 26th IEEE Computer Security Foundations Symposium. Tulane University, New Orleans, Louisiana, USA, 26-28 June 2013.

LICS 2013. The Twenty-Eighth Annual ACM/IEEE Symposium on Logic in Computer Science. Tulane University, New Orleans, Louisiana, USA, 25-28 June 2013.

FOSSACS 2013. The 16th Int.l Conf. on Foundations of Software Science and Computation Structures. (Part of ETAPS 2013.) Rome, Italy, March 2013.

SOFSEM 2013. 39th International Conference on Current Trends in Theory and Practice of Computer Science. Špindlerův Mlýn, Czech Republic, January 26–31, 2013.

CARDIS 2012. The Eleventh Smart Card Research and Advanced Application Conference. Graz, Austria, 28-30 November 2012.

QEST 2012. International Conference on Quantitative Evaluation of SysTems. London, UK, September 2012.

PPDP 2012. International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming. Leuven, Belgium, September 2012.

CONCUR 2012. 21st International Conference on Concurrency Theory. Newcastle, UK, September 2012.

CSF 2012. The 25th IEEE Computer Security Foundations Symposium. Cambridge MA, USA, June 2012.

POST 2012. First Conference on Principles of Security and Trust. Tallin, Estonia, March 2012.

Frank D. Valencia has been/is a member of the program committees of the following conferences and workshops:

CONCUR 2013. The 24th International Conference on Concurrency Theory. Buenos Aires, Argentina, 27-30 August 2013.

EXPRESS 2012: Combined 19th International Workshop on Expressiveness in Concurrency and 9th Workshop on Structural Operational Semantics. Newcastle upon Tyne, UK, 3 September 2012.

ICE 2012. The 5th International Workshop on Interaction and Concurrency Experience. Stockholm, Sweden, 16 June 2012.

Konstantinos Chatzikokolakis has been/is a member of the program committees of the following conferences and workshops:

ISPEC 2013: 9th International Conference on Information Security Practice and Experience.

QAPL 2013: 11th Workshop on Quantitative Aspects of Programming Languages.

ESOP 2012: 21th European Symposium on Programming.

TGC 2012: 7th International Symposium on Trustworthy Global Computing.

ISPEC 2012: 8th International Conference on Information Security Practice and Experience.

QAPL 2012: 10th Workshop on Quantitative Aspects of Programming Languages .

8.1.6. Participation in other committees

Catuscia Palamidessi serves in the following committees:

President of the selection committee for the EATCS Best Paper Award at the ETAPS conferences. Since 2006.

Member of the EAPLS PhD Award committee. Since 2010.

8.1.7. Organization of seminars

Frank D. Valencia, Luis Fernando Pino Duque, and Andrés Aristizábal are the organizer of the Comète-Parsifal Seminar. This seminar takes place weekly at LIX, and it is meant as a forum where the members of Comète and Parsifal present their current works and exchange ideas.

8.2. Service

Catuscia Palamidessi serves as:

Member of the Comité d'Orientation Scientifique et Technique, Groupe de travail Relation Internationales (COST-GTRI). Since November 2007.

Directrice adjointe du LIX, le Laboratoire d'Informatique de l'Ecole Polytechnique. Since April 2010.

Member of the Comité de These for Mathematics and Computer Science at the École Polytechnique. Since October 2007.

Reviewer for the projects proposal for the program PRIN, sponsored by the Italian MIUR ("Ministero dell'Istruzione, dell'Università e della Ricerca"). Since 2004.

Frank Valencia has served as:

Member of the Evaluation Committee of the LIX/Qualcomm postdoc grants for the year 2012.

8.3. Teaching

Master: Konstantinos Chatzikokolakis has been teaching the course "Concurrence" at the "Master Parisien de Recherche en Informatique" (MPRI) in Paris. Level M2. Total 12 hours.

Master: Miguel E. Andrés, Konstantinos Chatzikokolakis, and Catuscia Palamidessi have been teaching an advanced course on Quantitative Information Flow and on Differential Privacy at RIO 2012, the Summer School on Informatics Río Cuarto, Argentine. Total 20 hours. 13-18 February 2012.

Master. Frank D. Valencia has been teaching an advanced course on Process Modeling at Master Program in Computer Science of the Pontificia Universidad Javeriana de Cali, Colombia. Total 30 hours. A.Y. 2011-12.

PhD (2009-12) Andrés Aristizábal. Ecole Polytechnique. Grant CNRS/DGA. Title of the thesis: *Bisimulation Techniques and Algorithms for Concurrent Constraint Programming*. Defended on 17 October 2012. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD in progress (2012-) Marco Stronati. Ecole Polytechnique. Grant EDX Monge. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-). Ecole Polytechnique and Chinese academy of Science, Beijing, China. Co-supervised by Catuscia Palamidessi and Huimin Li.

PhD in progress (2011-) Nicolás E. Bordenabe. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Konstantinos Chatzikokolakis.

PhD in progress (2011-) Luis Fernando Pino Duque. Ecole Polytechnique. Grant Inria/DGA. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD in progress (2010-) Sophia Knight. Ecole Polytechnique. Grant Inria/CORDIS. Co-supervised by Catuscia Palamidessi and Frank D. Valencia.

PhD in progress (2009-) Ivan Gazeau. Ecole Polytechnique. Grant ANR. Co-supervised by Catuscia Palamidessi and Dale Miller.

8.3.1. PhD defenses

Catuscia Palamidessi has been reviewer for the thesis of the following PhD students:

James Jerson Ortiz Vega (Universidad del Valle, Cali, Colombia). Title of the thesis: *Formal Methods for the Specification and Verification of Distributed and Timed Systems*. Advised Juan Francisco Dias Frias. Defended in September 2013.

Thomas Given-Wilson (University of Technology, Sydney, Australia). Title of the thesis: *Concurrent Pattern Unification*. Advised by Barry Jay. Defended in August 2012.

Jacopo Mauro (University of Bologna, Italy). PhD thesis reviewer. Title of the thesis: *Constraints meet Concurrency*. Advised by Maurizio Gabbrielli. Defended in April 2012.

Catuscia Palamidessi has been member of the committee at the HDR defense of Daniele Varacca, University of Paris VII, December 2012.

CONTRAINTES Project-Team

9. Dissemination

9.1. Scientific Animation

- Grégory Batt has organized an international workshop on Design, optimization and control in systems and synthetic biology at ENS Paris during two days (15 speakers, 230 registered participants, 14 nationalities).

  Grégory Batt's invited seminars:
  - Summer school Naturel et artificiel: le vivant et ses représentations, Berder, Apr 03, invited talk
  - Model-based analysis and control of cellular processes workshop, Purdue, IN, USA, Oct 09, contributed talk
  - Perspectives en Biologie de Synthèse, Aviesan/Allenvi workshop, Paris, Dec 11, invited talk

  He has been a member of the Program Committee of the JOBIM'12 conference. He was a reviewer for Bioinformatics, IEEE Transactions on Computational Biology and Bioinformatics, and Biosystems.

- François Bertaux was invited to short working visits at the Weiss Lab (MIT, Boston, USA) - March and May/June.

- Xavier Duportet's invited seminar and contributed poster presentations:
  - La Biologie de Synthèse, Bar des Sciences, Paris, April 06, invited talk
  - SynBerc retreat, MIT, USA, October 11, poster

  He has been involved in technological transfer activities:
  - Provisional patent application: High-throughput discovery of recombinase sites towards the engineering of recombinase specificity
  - Gen9 Inaugural G-Prize, 3rd place winner, Cambridge, MA

  He is a member of Synthetic Biology Scientific Committee at Alliance pour la recherche et l'innovation des industries de santé (ARIIS), Paris.

- François Fages is a member of
  - Editorial Board of RAIRO Operations Research,
  - Steering Committee of the International Conference series on Computational Methods in Systems Biology (CMSB).

  He is a member of the Scientific Advisory Boards of
  - the Center for Systems Biology at Edinburgh, Scotland,
  - the Doctorate School Frontières du Vivant of the University Paris Descartes
  - the Laboratoire d'Informatique Fondamentale, University of Orléans.

  and a member of the
  - "Comité de pilotage" of the OSEO BioIntelligence project, coordinated by Dassault-Systèmes

François Fages has co-organized the fourth international workshop on "Bin packing and placement constraints" BPPC'12 associated to CPAIOR'12 in Nantes, June 2012.

He was member of the program committees of CHR'12, CMSB'12, CS2BIO'12, FHIES'12, ICORES'12, SASB'12 and WCB'12. He has reviewed articles for the following journals: ACM Transactions on Computational Logics, Artificial Intelligence, Constraints, BioMedCentral systems biology, Constraints, PLOS One, Rairo OR.

François Fages was reviewer of research grants for

– the Agence Nationale de la Recherche (ANR),

– the Royal Society (London),

– and the Swiss National Science Foundation (SNSF).

Invited seminars:

– Dagstuhl's seminar on formal methods for chemical reaction networks, Schloss Dagstuhl, Germany, October 2012.

– Formal methods in systems biology workshop, associated to CAV'12, Berkeley, USA, July 2012.

– Symposium Biointelligence, Sophia-Antipolis, July 2012.

– CP meets CAV workshop, Turunc, Turkey, June 2012.

– 25 ans du LIFO, Orléans, March 2012.

- Thierry Martinez acted as a member of the Program Committee of CHR'12.

- Sylvain Soliman acted as reviewer for CMSB'12 and BMC Systems Biology, as member of the Program Committee of JFPC'12. He was also expert/reviewer for the French PEPS biologie-mathématiques-informatique call (CNRS/INSERM/Inria).

  He gave an invited seminar at Institut Curie's bioinformatics team. "Reaction Graphs to Regulatory Networks - Theory to practice".

- Szymon Stoma was invited to short working visits at the Weiss Lab (MIT, Boston, USA) - March and May/June.

- Denis Thieffry is currently

  – member of the Comité Scientifique Sectoriel of the Department *Biologie et Santé* of the ANR;

  – member of the Comité de Pilotage of the LabEx MemoLife (involving teams from IBEns, Collège de France, and ESPCI);

  – member of the CNRS/INSERM ATIP/Avenir Scientific Committee (young group leader grant scheme);

  – member of the board of the PhD Program Complexity in Post-Genomic Biology of the University of Torino;

  – member of the program committees for ECCB-ISMB, JOBIM, CMSB, and SASB;

  – Editor of BioSystems;

  – Associated Editor of PLoS Computational Biology;

  – Adviser for the PLoS Biology Education series.

- Jannis Uhlendorf gave an invited seminar at the BioComputing group of the Laboratoire d'Informatique Fondamentale de Lille on Real-time control of gene expression in February 2012.

9.2. Teaching - Supervision - Juries

9.2.1. *Teaching*

Contraintes is affiliated to the Doctoral school of Mathematical Science of the University Paris Diderot, and to the interdiciplinary Doctoral school "Frontières du Vivant" of the University Paris Descartes.

The following courses have been given by members of Contraintes:

Summer school Scientific Trends at the Interfaces: Biomathematics - Bioinformatics, Roscoff, Grégory Batt (6h) and François Bertaux (6h).

Master M2 course C2-19 on *Computational Methods for Systemic and Synthetic Biology*, Master Parisien de Recherche en Informatique (MPRI) François Fages (responsible, 12h), Grégory Batt (12h), Denis Thieffry (12h).

Master: Cell Systems Biology master curriculum at the Ecole Normale Supérieure, Paris. Denis Thieffry (coordinator).

Master M2 course C2-35-1 on *Constraint Programming*, Master Parisien de Recherche en Informatique (MPRI) Sylvain Soliman (responsible, 24h) [end of the 2011-2012 academic year].

Master M1 course on *Computational Biology*, Master Approches Interdisciplinaires du Vivant (AIV), Grégory Batt (coordinator, 40h).

Master M1 course on Synthetic Biology, AgroParisTech, Xavier Duportet (12h).

Master M1 course on Synthetic Biology, Faculté de Médecine de Paris, Xavier Duportet (4h).

Licence L2 Cours/TD *Informatique*, Université de Paris Dauphine, Faten Nabli (72h).

Science, Innovation and Entrepreneurship non for profit organization: 4 conferences (400 people), Paris, Xavier Duportet (12h)

9.2.2. Supervision

PhD in progress : François Bertaux, Université Pierre et Marie Curie, Paris, Sept 2011, Dir. Dirk Drasdo (EPI BANG) and Grégory Batt

PhD in progress : Xavier Duportet, Université Paris Descartes, Paris, Oct 2010, Dir. Grégory Batt, François Fages and Ron Weiss (MIT)

PhD in progress : Steven Gay, Université Paris Diderot, Paris, Oct 2009, Dir. François Fages and Sylvain Soliman,

PhD in progress : David Fournier, Université Paris Diderot, Paris, Oct 2011, Dir. François Fages and Denis Mulard (General Electric),

PhD in progress : Jean-Baptiste Lugagne, Université Paris Diderot, Paris, Oct 2012, Dir. Grégory Batt, François Fages and Pascal Hersen (MSC)

PhD in progress : Artemis Llamosi, Université Paris Diderot, Paris, Nov 2012, Dir. Grégory Batt, Jean-Marc di Meglio and Pascal Hersen (MSC)

PhD in progress : Thierry Martinez, Université Paris Diderot, Paris, Oct 2009, Dir. François Fages,

PhD in progress : Faten Nabli, Université Paris Diderot, Paris, Oct 2009, Dir. François Fages and Sylvain Soliman

PhD in progress : Pauline Traynard, Université Paris Diderot, Paris, Oct 2012, Dir. François Fages and Denis Thieffry (ENS)

PhD in progress : Jannis Uhlendorf, Université Paris Diderot, Paris, Oct 2009, Dir. Grégory Batt, François Fages and Pascal Hersen (MSC)

PhD in progress : Luma Vittorino, Université Paris Diderot, Paris, Oct 2012, Dir. François Fages,

9.2.3. Juries

PhD Thesis committee of Roberto Amato, Ankita Chaurasia, Francesca Fioretti, Filippo Menolascina, and Alessandra Vigilante, University of Naples, Italy, Member Grégory Batt.

HDR of Khallil Djelloul, University of Orléans. Reviewer François Fages.

PhD Thesis defense of Andrés A. Aristizàbal, Ecole Polytechnique. Chairman François Fages.

PhD Thesis committee of Adrien Basso-Blandin, University of Evry. Member François Fages.

PhD Thesis defense of Emmanuel Halloit, University of Nice, Villefranche sur Mer, décembre 2012. Member Denis Thieffry.

PhD Thesis defense of Guillaume Baptist, Université Joseph Fourrier, Grenoble, août 2012. Reviewer Denis Thieffry.

PhD Thesis defense of Mohamed Hedi Ben Amor, Université Joseph Fourrier, Grenoble, juillet 2012. Member Denis Thieffry.

9.3. Popularization

Our PNAS article attracted the attention of the media. Articles entitled "Ils contrôlent le vivant avec des ordinateurs !", "Des cellules qui obéissent au doigt et à l'oeil", "Focusing the phenotype - Controlling genetic expression through external feedback" appeared in l'Humanité Dimanche, le journal du CNRS, and Phys.org. Also, Grégory Batt participated to the radio program "Autour de la question" (RFI).

Two posters, "(Re)programmer le vivant" and "Des cellules pilotées par ordinateur", were presented during the Fête de la science to a broad audience during two days by Grégory Batt.

Denis Thieffry has two books in press:

- Thieffry D. Gene networks, logical modelling, and regulatory motifs entries. In: Hancock JM, Zvelebil MJ (eds). Dictionary of Bioinformatics and Computational Biology. New York: John Wiley & Sons.

- Faur A, Thieffry D. Cell cycle modelling using logical rules. In: Dubitzky W, Wolkenhauer O, Cho K-H, Yokota H (eds.) Encyclopedia of Systems Biology. Springer.

DEDUCTEAM Team

7. Dissemination

7.1. Scientific Animation

Gilles Dowek has been a PC member of LICS, CSL, TAMC, and ICECCS. He is a member of the Scientific Board of the *Société Informatique de France*. He is a member of the *Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene*. He is Deputy scientific director of Inria.

Catherine Dubois has been a PC member of TAP and AFADl. She has been the chair of the TAP steering committee since May 2012.

7.2. Teaching - Supervision - Juries

7.2.1. Teaching activities

Olivier Hermant has taught at ISEP four engineering courses: Preparation to the ACM programming contest, Data bases, Formal methods, and Algorithmics.

Guillaume Burel has taught at ENSIIE five courses: Logic, Formal languages, Compilation, and Semantics of programming languages.

Alejandro Díaz-Caro has been teaching assistant at Paris 10 for four courses: in Mathematics (in two different degrees) and in Methodology of measure in social sciences.

Pierre Néron has been a teaching assistant in Polytech' Jussieu for two courses: Project in C and Introduction to networks.

Gilles Dowek has taught in MPRI a course: Foundations of proof systems. He has coordinated a textbook for high school students [39]. He is a member of the Scientific board of *La main à la pâte*.

7.2.2. Ph.D. supervision

Olivier Hermant supervises the theses of Ronan Saillard, Giang Le Truong, and Vivien Maisonneuve.

Catherine Dubois and David Delahaye supervise the thesis of Mélanie Jacquel and Pierre Nicolas Tollitte.

Catherine Dubois and Francois Pessaux (ENSTA) supervise the thesis of Vincent Benayoun.

Catherine Dubois supervises the research internship of Raphaël Cauderlier.

Guillaume Burel and Gilles Dowek supervise the theses of Ali Assaf and Simon Cruanes.

Gilles Dowek supervises the thesis of Pierre Néron.

7.2.3. Supervision of Masters internship

Catherine Dubois and Olivier Hermant have supervises the Masters internship of Raphaël Cauderlier.

Olivier Hermant and Mathieu Boespflug have supervised the Masters internship of Quentin Carbonneaux.

Guillaume Burel and Gilles Dowek have supervised the Masters internship of Ali Assaf.

Gilles Dowek and Pierre Néron have supervised the Masters internship of Raphaël Bost.

7.2.4. Juries

Gilles Dowek has been a member of the Jury of Vincent Demange. he has been a member of the Jury of the habilitations of Frédéric Blanqui and Sylvain Conchon.

Catherine Dubois has been a member of the jury of Maximiliano Cristia and a member of the jury of Ophaina Taofifenua.

7.3. Popularization

Gilles Dowek has given a talk at the Centre d'Alembert, at the Lycée Jacquard in Paris and at the Lycée Montaigne in Bordeaux.

<div align="center">

FORMES Team

</div>

9. Dissemination

9.1. Scientific Animation

Frédéric Blanqui is member of the steering committe of the international conference on rewriting techniques and its applications (RTA).

Frédéric Blanqui was member of the program committee of the 6th International Workshop on Higher-Order Rewriting (HOR'12).

Jean-Pierre Jouannaud was member of the program committee of WOLLIC'2012.

Jean-Pierre Jouannaud is a member of the steering committee of LICS.

Jean-Pierre Jouannaud is a member of the Advisory Committee of Academia Sinica, Taipei.

Jean-Pierre Jouannaud is a member of the committee for the Ackermann prize (2011–2013).

Jean-Pierre Jouannaud was a member of the committee for the LICS test of time award (2012).

Vania Joloboff was invited speaker at China Open Source Week in Nanjing.

Vania Joloboff was invited speaker at a professional embedded systems workshop in Tokyo.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Ming Gu is the director of the School of Software, Tsinghua. She teaches at all levels.

Last year undergraduate: Jianqi Li, An Introduction to Theories of Software, 16 hours, L1, Tsinghua University, China

Licence : Jean-François Monin, Introduction to Interactive Proof of Software, 50 hours, L3, Tsinghua University, China

This course is expected to attract students in the FORMES group via the local PhD program; already one of them (2009) is currently a PhD student of Jean-Pierre Jouannaud, another (2010) in is the PhD track with Gu Ming and 2 others (2010) work with Jean-François Monin and Vania Joloboff.

Licence : Jean-François Monin, Introduction to Functional Programming, 25 hours, L3, Beijing Jiatong University, China

Master: He Fei, Formal verification for software systems, 32 hours, Tsinghua University, China

Master: Jianqi Li, The Formal Semantics of Programming Languages, 32 hours 2012, M1, Tsinghua University, China

Master : Jean-François Monin, Complements on Coq, 25 hours, M1-M2, Beijing University (PKU), China

Doctorate : Frédéric Blanqui, Introduction to domain theory and topology, 3 hours, ISCAS, Beijing, China

Doctorate : Jean-François Monin, Coq Summer School, 20 hours, ECNU Shanghai, China

9.2.2. Supervision

PhD & HdR :

PhD in progress : Jiaxiang LIU, Decreasing diagrams for confluence, Sept. 2011 Jean-Pierre Jouannaud

PhD in progress : Qian WANG, A Complete Formalization of Coq Modulo Theory, Sept. 2010, Jean-Pierre Jouannaud

PhD in progress : Xiaomu SHI, Formalisation and Proof of an Instruction Set Simulator, nov. 2009, Jean-François Monin and Vania Joloboff

PhD in progress : Kim Quyen LY, Automated Verification of Termination Certificates, nov. 2010, Frédéric Blanqui

9.2.3. Juries

Jean-Pierre Jouannaud: ENS-Cachan, habilitation, Florent Jacquemard (rapporteur)

Jean-François Monin: Paris-7, PhD, Stéphane Glondu (rapporteur)

Jean-François Monin participated to the recruitment of Chinese students for the polytechnic engineering schools of Grenoble, Marseille, Montpellier and Nice.

9.3. Popularization

Jean-Pierre Jouannaud gave presentations about formal proofs and related topics at Tsinghua, one in the department of applied mathematics in november 2011, and one in the department of computer science in june 2011.

Vania Joloboff has given presentations about simulation at

- Shanghai Fudan University
- Guangzhou Normal University
- a workshop in Japan about Trustworthy Embedded Systems

Jean-François Monin gave presentations about formal methods and our research at FORMES to Jiaotong (Shanghai) in June 2011, UPC (Qingdao) in October 2012, HIT (Harbin) in November 2012 and ECNU (Shanghai) in December 2012.

Jean-François Monin initiated formal agreements between several Chinese universities (Wuhan university, Beijing Jiaotong, UPC, HIT) and the Polytech Group or UJF, and developed the existing formal cooperation between Beihang and UJF.

GALLIUM Project-Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Conference organization

Didier Rémy co-chaired the OCaml Users and Developers Workshop (OUD 2012), affiliated with ICFP 2012, which took place in Copenhagen, Denmark in September 2012.

Didier Rémy is organizing the next meeting of IFIP working group 2.8 "Functional programming", which will take place in Aussois, France, in October 2013.

9.1.2. Editorial boards

Xavier Leroy was co-editor in chief of the Journal of Functional Programming until March 2012, when he stepped down at the end of his 5-year term.

Xavier Leroy is a member of the editorial boards of Journal of Automated Reasoning, Journal of Functional Programming, and Journal of Formalized Reasoning.

9.1.3. Program committees

Damien Doligez was a member of the program committee of the International Workshop on the TLA+ Method and Tools 2012 (TLA 2012), a satellite event of Formal Methods 2012 (FM 2012)

Xavier Leroy was a member of the program committees of the ACM symposium on Principles of Programming Languages (POPL 2013) and of the European Symposium on Programming (ESOP 2013). He was a member of the external review committee for the ACM conference on Programming Languages Design and Implementation (PLDI 2013).

François Pottier was a member of the program committees of the ACM workshops on ML (ML 2012), on Higher-Order Programming with Effects (HOPE 2012), and on Programming Languages meets Program Verification (PLPV 2013). He was a member of the external review committee for the ACM symposium on Principles of Programming Languages (POPL 2013).

Na Xu was a member of the program committee of the ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation (PEPM 2013).

9.1.4. Steering committees

Xavier Leroy is a member of the steering committees for the Certified Programs and Proofs (CPP) conference and for the ACM PLPV workshop.

François Pottier is a member of the steering committee for the ACM TLDI workshop.

Didier Rémy is a member of the steering committee of the OCaml Users and Implementors Workshop.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: "Algorithmique et programmation" (INF431), 13h30, L3, École Polytechnique, France. Lecturer: François Pottier (*professeur chargé de cours*).

Licence: "Algorithmique et programmation", 40h, L3, École Polytechnique, France. Teaching assistant: Jonathan Protzenko.

Licence: "Bases de données", 26h, L1, U. Paris Diderot, France. Teaching assistant: Julien Cretin.

Licence: "Principe de fonctionnement des machines binaires", 33h, L1, U. Paris Diderot, France. Teaching assistant: Julien Cretin.

Licence: "Travaux dirigés de Caml Light", 36h, L1 (classes préparatoires MPSI), Lycée Louis-le-Grand, France. Teaching assistant: Gabriel Scherer.

Master: "Functional programming and type systems", 30h, M2, MPRI master (U. Paris Diderot and ENS Paris and ENS Cachan and Polytechnique), France. Lecturers: Xavier Leroy (12h) and Didier Rémy (18h).

Master: "Modal Web", 36 hours, M1, École Polytechnique, France. Teaching assistant: Jonathan Protzenko.

Doctorat: "Proving a compiler: mechanized verification of program transformations and static analyses", 7h, Oregon Programming Languages Summer School, USA. Lecturer: Xavier Leroy.

9.2.2. *Supervision*

PhD: Nicolas Pouillard, "A unifying approach to safe programming with first-order syntax with binders", U. Paris Diderot, defended January 13th, 2012, supervised by François Pottier.

PhD: Tahina Ramananandro, "Mechanized formal semantics and verified compilation for C++ objects", U. Paris Diderot, defended January 10th, 2012, supervised by Xavier Leroy.

PhD in progress: Julien Cretin, "Coercions in typed languages", since December 2010, supervised by Didier Rémy.

PhD in progress: Alexandre Pilkiewicz (currently employed by Google in New York), "Verifying polyhedral optimizations", U. Paris Diderot, since December 2008, supervised by François Pottier

PhD in progress: Jonathan Protzenko, "Fine-grained static control of side effects", U. Paris Diderot, since September 2010, supervised by François Pottier.

PhD in progress: Gabriel Scherer, "Modules and mixins", U. Paris Diderot, since October 2011, supervised by Didier Rémy.

PhD in progress: Jacques-Henri Jourdan, "Formal verification of static analyzers for critical embedded software", U. Paris Diderot, since September 2012, supervised by Xavier Leroy.

9.2.3. *Juries*

Xavier Leroy was reviewer (*rapporteur*) for the Ph.D. of Robert Dockins (Princeton University, August 2012), Antonis Stampoulis (Yale University, October 2012), and Delphine Demange (ENS Cachan Bretagne, October 2012). He was a member of the Ph.D. jury of Ricardo Bedin França (U. Toulouse, April 2012). Xavier Leroy chaired the Habilitation jury of Fabrice Rastello, ENS Lyon, December 2012.

François Pottier was an external examiner for the Habilitation defense of Etienne Lozes (École Normale Supérieure de Cachan, July 3, 2012) and for the Ph.D. defense of Jérémy Planul (École Polytechnique, February 8, 2012), Thibaut Balabonski (Université Paris Diderot, November 16, 2012), and Antoine Madet (Université Paris Diderot, December 6, 2012).

9.3. Popularization

Jacques-Henri Jourdan participated in the organization of the *Castor* computer science contest (http://castor-informatique.fr/). This contest aims at making computer science more popular in French high schools and junior high schools. It attracted over 90,000 participants.

Xavier Leroy gave a popular science talk on critical avionics software at the December 2012 "Jam session" meeting of Inria Alumni.

Jonathan Protzenko, along with two other PhD students, is curating the Junior Seminar in Rocquencourt, where he coaches other PhD students into presenting their work in front of a friendly audience.

Gabriel Scherer set up a research blog for the Gallium project-team, to highlight small chunks of work of the team members in an informal and popularized style. For example, Valentin Robert, Thomas Braibant and Jacques-Henri Jourdan described various aspects of their interaction with the Coq proof assistant, some of which eventually resulted in small improvements integrated by the Coq development team. Articles are published approximately once a week, and the blog gets on average 500 visits a day.

MARELLE Project-Team

7. Dissemination

7.1. Scientific Animation

- We organized the MAP spring school on the formalization of mathematics, March 12-16, 2012, at Inria Sophia Antipolis. This school had 65 attendants and 5 invited speakers: G. Gonthier (Microsoft Research, Prize the EADS foundation), T. Hales (University of Pittsburgh), J. Rubio (Universidad de la Rioja), B. Spitters (Radboud University), and V. Voevodsky (Institute for Advanced Study, Fields Medal). The local organization was supervised by Yves Bertot and included a strong investment by Nathalie Bellesso and Agnès Cortell, from Inria's service for scientific events. Yves Bertot, Laurence Rideau, and Laurent Théry also taught at this school.
- Yves Bertot participated as a lecturer in the asian-pacific summer school on formal methods, July 16-20, at East China Normal University in Shanghai. He gave 6 lectures and supervised laboratory sessions.
- Yves Bertot and Patrick Rambert released a multi-media course on the Coq system, consisting in more than 8 hours of recorded courses available at http://fuscia.inrialpes.fr/cours/coq/.
- members of the project participated in the program committees of PXTP (Proof Exchange for Theorem Proving), PAAR (Practical Aspects of Automated Reasoning), ITP (Interactive Theorem Proving).

7.2. Teaching - Supervision - Juries

7.2.1. Teaching

Licence : Laurence Rideau, introduction to programming in CAML, Classe préparatoire MP* (L2 level), Lycée Masséna, Nice

Master : Benjamin Grégoire, "Verification and Security", 18 ETD, M2, University of Nice, France

Master : Yves Bertot, "Verification of proofs and programs", 27 ETD, University of Nice, France

Master : Laurent Théry, "Introduction to Coq", 3 ETD, Ecole des Mines, Sophia Antipolis, France

Master : Laurent Théry, "Formalization of floating point arithmetic", Ecole Normale Supérieure de Lyon, France

Doctorate : Yves Bertot, "Introduction to formalized mathematics", 30ETD, Inria Sophia Antipolis, France

Doctorate : Laurence Rideau, "Introduction to formalized mathematics", 30ETD, Inria Sophia Antipolis, France

Doctorate : Laurent Théry, "Introduction to formalized mathematics", 30ETD, Inria Sophia Antipolis, France

Doctorate : Yves Bertot, "Formal verification with Coq", 50 ETD, East China Normal University, Shanghai, China.

7.2.2. Supervision

PhD & HdR :

PhD : Sylvain Heraud, "Verification Semi-automatique de primitives cryptographiques", University of Nice Sophia Antipolis, March 12, 2012 (thesis started in October 2008), supervisor : Benjamin Grégoire.

PhD in progress : Michaël Armand, "Application de la certification de résultats à l'automatisation de preuves interactives", started in October 2009, supervisors: Laurent Théry and Benjamin Grégoire.

PhD in progress : Guillaume Cano, "Une formalisation adaptable de l'algèbre linéaire", started in October 2010, supervised by Yves Bertot.

PhD in progress : Maxime Dénès, "Description formelle d'algèbre linéaire pour l'algorithmique rapide", started in September 2010, supervised by Yves Bertot.

7.2.3. Juries

+ Yves Bertot was a reviewer for the PhD theses of Celia Picard (U. Toulouse) and Erik Martin-Dorel (ENS Lyon) and an examiner for the thesis of Francesco Bongiovanni (U. Nice).

+ Laurent Théry was an examiner for the thesis of Thomas Braibant (U. Grenoble) and for the Licenciate degree of Anders Mörtberg (U. Göteborg, Sweden).

7.3. Popularization

- Laurence Rideau took part in a presentation of research topics for students from "classes préparatoires" at Inria Sophia Antipolis Méditerranée.

<div style="text-align:center">

MEXICO Project-Team

</div>

8. Dissemination

8.1. Scientific Animation

8.1.1. Benedikt Bollig

was the organizer and a PC member of the 4rd Young Researchers Workshop on Concurrency Theory (YR-CONCUR), which was co-located with CONCUR'12. He was a PC member of the International Workshop on Interactions, Games and Protocols (IWIGP'12). Moreover, he served as a reviewer for numerous international conferences and journals. He also was a member of the *commission scientifique* Inria Saclay.

8.1.2. Thomas Chatain

was a member of the program committee of ACSD'12 (*International Conference on Application of Concurrency to System Design*). He was a member of a selection committee at CNAM Paris in 2012, and participated in the organization and presentation of the one-day Petri net tutorial on unfoldings at the *international conference on the application and theory of Petri nets* in Hamburg, June 2012.

8.1.3. Paul Gastin

is co-head (with Madhavan Mukund) of the new International Associated Laboratory (LIA) INFORMEL (INdo-French FORmal Methods Lab). This LIA was created in January 2012 by an agreement between CNRS, ENS Cachan, University Bordeaux 1 on the french side and the Chennai Mathematical Institute, the Institute of Mathematical Sciences of Chennai, and the Indian Institute of Science of Bangalore on the Indian side.

He is the head of the computer science department of ENS Cachan.

Paul Gastin is an associate editor of the Journal of Automata, Languages and Combinatorics.

He is on the Advisory Board of the EATCS-Springer book series

- Monographs in Theoretical Computer Science,
- Texts in Theoretical Computer Science.

He was a member of the program committees of LATA 2012 (Language and Automata Theory and Applications) and CONCUR 2012 (International Conference on Concurrency Theory).

He was an invited speaker at the 17th International Conference on Implementation and Application of Automata (CIAA'12).

He was a member of 3 selection committees (Cachan, Nancy and Orléans).

8.1.4. Stefan Haar

is an associate editor for the journal *Discrete Event Dynamic Systems: Theory and Application*, and was on the program committees of *SAFEPROCESS 2012* and *PNSE 2012*. He participated in the organization and presentation of the one-day Petri net tutorial on unfoldings at the *international conference on the application and theory of Petri nets* in Hamburg, June 2012 Stefan is the correspondent for Inria's *DRI* (international relations service) for the Saclay center, and ipso facto member of the GTRI (working group on international relations) of Inria's COST.

8.1.5. Serge Haddad

has been a member of the steering committee of the *International Conference on Application and Theory of Petri Nets (ICATPN)* since 2001. He gave a tutorial on timed and stochastic Petri nets, and was co-president of the program committee of ICATPN 2012; he was also co-president for the tutorials at the 18th Int. Symp. on Formal Methods (FM) 2012, Paris, France, and member of the program committee of the Workshop on Research and Use of Multiformalism Modeling Methods of QEST, September 2012, London, UK. He is a founding member of the research group *MeFoSyLoMa* and co-chair of the software project *COSYVERIF*. He was one of the evaluators in the Evaluation AERES of the *Cedric* Laboratory, and is a member of the selection committees of the universities Paris VI and Nancy.

8.1.6. Stefan Schwoon

was a member of the program committee of GRAPHITE'12 (First Workshop on GRAPH Inspection and Traversal Engineering). and of the MOVEP 2012 winter school. He gave a tutorial on unfolding and partial-order techniques at CEA LIST in January.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Here we present the teaching activities of PhD students and *researchers*; note that in addition to the classes here, four team members (Th. Chatain, P. Gastin, S. Haddad and S. Schwoon) are full-time professors of ENS Cachan and fulfill their teaching obligations there.

Master : Sandie Balaguer, Programmation en C, 32, M1, U.F.R d'Informatique de Paris 7, France

Master : Benjamin Monmege, Probabilistic Aspects of Computer Science, 10h, M1, ENS de Cachan, France

Master : Benoît Barbot, Projet de programmation réseau, 30h, M1, ENS Cachan, France

Master : Benedikt Bollig, Modeling and verification of real-time distributed systems, 12, M2, MPRI, France

Ecole d'Ingénieur: Hernán Ponce de León, Algorithmique et Programmation, 32, 3e année (equivalent L3), Ecole Centrale Paris, France

Master : Stefan Haar, Verification (VSFR), 12, M2, UPMC, France

Master : Stefan Haar, Modelisation et optimisation (MOPS), 12, M2, Université d'Evry, France

Agrégation : Stefan Haar, Algorithmique , 42.5, Agrégation option informatique, ENS Cachan

Master : César Rodríguez, Projet de programmation réseau, 30h, M1, ENS Cachan, France

Agrégation : César Rodríguez, TP programmation, 24h, Préparation à l'agrégation, ENS Cachan, France

Licence : Aiswarya CYRIAC, Algorithmique avancée, 60, niveau L3, ENS de Cachan, France

Licence: Benoît Barbot , Mathématiques Discrètes, 22.5 , L3 , ENS Cachan, France

Licence : Benjamin Monmege, Machine learning, 60h, L3, ENS de Cachan, France

8.2.2. Supervision

PhD & HdR :

PhD: Sandie Balaguer, Concurrency in Real-Time Distributed Systems, ENS Cachan, December 13, 2012, supervised by Stefan Haar and Thomas Chatain.

PhD: Hilal Djafri, Numerical and Statistical Approaches for Model Checking of Stochastic Processes, ENS Cachan, June 19, 2012, supervised by Serge Haddad.

PhD in progress: Hernán Ponce de Léon, Testing of concurrent systems using event structures, ENS Cachan, supervised by Stefan Haar and Delphine Longuet (Paris XI)

PhD in progress: César Rodríguez, *Contextual Petri Nets and Applications*, begun in September 2010,. supervised by Stefan Schwoon

PhD in progress: Aiswarya Cyriac, *Temporal logics for concurrent recursive programs*, begun in September 2010, supervised by Benedikt Bollig and Paul Gastin.

PhD in progress: Benjamin Monmege, *Specification and verification of qualitative properties and applications to queries for XML documents*, begun in September 2010, supervised by Benedikt Bollig and Paul Gastin.

PhD in progress: Benoît Barbot, *Rare event handling in statistical model checking*, begun in September 2011, Serge Haddad and Claudine Picaronny (ENS Cachan).

8.2.3. *Juries*

8.2.3.1. *Thomas Chatain*

participated , as examinator and co-supervisor, in the PhD committee of Sandie Balaguer ([43], December 13, 2012).

8.2.3.2. *Paul Gastin*

was president of the committee for the HDR of Daniele Varacca at *Université Paris Diderot*.

8.2.3.3. *Stefan Haar*

was president of the Ph D committees of Hilal Djafri [44] at ENS Cachan (June 19, 2012)and Hoang-Thach Nguyen at Paris VII (April 18, 2012), and member (as the thesis supervisor) of the PhD committee of Sandie Balaguer ([43], December 13, 2012). He will be a reviewer for the thesis of Elisabeta Mangioni at University of Milan-Bicocca in Italy.

8.2.3.4. *Serge Haddad*

was examinator and thesis supervisor in the Ph D committee of Hilal Djafri [44] at ENS Cachan (June 19, 2012). He also was a reviewer for the thesis of H. Schonenberg at Eindhoven University, mai 2012, and member of the PhD Committees of L. Jezequel (University of Rennes, november 2012, and M. Lauer at INP Toulouse, june 2012.

8.2.3.5. *Stefan Schwoon*

participated in the *jury de mi-parcours* of Ala Eddine Ben Salem, PhD student at LIP6.

PAREO Project-Team

8. Dissemination

8.1. Scientific Animation

- Jean-Christophe Bach:
  - Reviewer for SLE 2012 (5th International Conference on Software Language Engineering)
- Horatiu Cirstea:
  - PC member of RuleML 2012 (International RuleML Symposium on Rule Interchange and Applications).
  - Steering committee of RULE.
  - Responsible for the Master speciality "Logiciels: Théorie, méthodes et ingénierie".
- Claude Kirchner:
  - Keynote speaker of RTA 2012 (23rd International Conference on Rewriting Techniques and Applications): "Rho-Calculi for Computation and Logic".
- Sergueï Lenglet:
  - Presentation at "Journées communes LTP - LAC - LaMHA"
- Pierre-Etienne Moreau:
  - Member of the board of the Doctoral School in Computer Science and Mathematics.
  - Member of the GDR–GPL (CNRS Research Group on Software Engineering) board.
  - Head of the local committee for Inria "détachements" and "délégations".
  - Head of the Computer Science department at Ecole des Mines de Nancy.
  - PC member of RTA 2012 (23rd International Conference on Rewriting Techniques and Applications), SLE 2012 (5th International Conference on Software Language Engineering), and WRLA 2012 (9th International Workshop on Rewriting Logic and its Applications)
- Sorin Stratulat:
  - PC Member of SYNASC'12 (14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing), IAS'12 (8th International Conference on Information Assurance and Security), and CISIS'12 (5th International Conference on Computational Intelligence in Security for Information Systems).
  - Invited Speaker at PAS'12 (International Seminar on Program Verification, Automated Debugging and Symbolic Computation).
  - Member of the LITA Laboratory Council.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Horatiu Cirstea, Structures de données, 20h, L3, Université de Lorraine, Nancy

Licence : Sergueï Lenglet, Algorithmique et strutures de données, 110h, L1, L2, IUT Charlemagne, Nancy

Licence : Sergueï Lenglet, Bases de données, 60h, L1, IUT Charlemagne, Nancy

Licence : Sergueï Lenglet, Analyse et conception de systèmes d'information, 20h, L2, IUT Charlemagne, Nancy

Licence : Pierre-Etienne Moreau, Tronc Commun d'Informatique, 35h, L3, École des Mines de Nancy

Licence : Christophe Calvès, Certificat Informatique et Internet, 40h, L1, Université de Lorraine, Nancy

Master : Horatiu Cirstea, Analyse et conception de logiciels, 100h, M1, Université de Lorraine, Nancy

Master : Horatiu Cirstea, Génie logiciel avancé, 30h, M2, Université de Lorraine, Nancy

Master : Pierre-Etienne Moreau, Software Engineering, 15h, M1, École des Mines de Nancy

Master : Pierre-Etienne Moreau, Bootcamp OO Programming, 45, M1, École des Mines de Nancy

Master : Pierre-Etienne Moreau, Research project, 30h, M2, École des Mines de Nancy

8.2.2. *Supervision*

PhD : Cláudia TAVARES, "Un système de types pour la programmation par réécriture embarquée", Université de Lorraine, March 2nd 2012, Claude Kirchner et Pierre-Etienne Moreau

PhD : Vincent DEMANGE, "Vers un calcul des constructions pédagogiques", Université de Lorraine, December 7th 2012, Sorin Stratulat et Loïc Colson

PhD in progress : Jean-Christophe BACH, "Transformation de modèles et certification", November 1st 2010, Pierre-Etienne Moreau

8.2.3. *Juries*

Pierre-Etienne Moreau:

PhD committee of Aurélien Monot, "Vérification de contraintes temporelles de bout-en-bout dans le contexte AutoSar", Nancy 2012

PhD committee of Luc Engelen, "From Napkin Sketches to Reliable Software", Eindhoven 2012

PhD reviewer of Pengfei Liu, "Intégration de politiques de sécurité dans des systèmes ubiquitaires", Bordeaux 2013

PhD committee of Laurent Wouters, "Multi-Domain Expert-User Modeling Infrastructure", Paris 2013

8.3. Popularization

Jean-Christophe Bach participated to scientific mediation by proposing several activities to demonstrate the *algorithmic thinking* at the core of the Computer Science without requiring any computer or even electric devices. These activities are the first part of the CSIRL (Computer Science In Real Life) project which aims to popularize computer science and to initiate children, school students and non-scientists into this domain. These activities were presented during the high school students welcome at LORIA and Inria - Nancy Grand Est, and also during APMEP [1] days.

Jean-Christophe Bach was also involved in popularization activities with Interstices [2] by writing short debunking articles ("Idées reçues") for non computer scientists about Church's thesis and Turing's work.

---

[1] http://www.apmep.asso.fr/
[2] http://interstices.info

PARSIFAL Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. Organization

Dale Miller served as Program Committee Chair for the following three meetings: CPP 2012: Second International Conference on Certified Programs and Proofs, 13-15 December, Kyoto, Japan; IJCAR 2012: International Joint Conference on Automated Reasoning, Manchester, UK, June; FICS 2012: Fixed Points in Computer Science (a satellite workshop of ETAPS 2012), Tallinn, Estonia, 24 March.

Dale Miller served on the Program Committees of the following three meetings: LFMTP'12: Workshop on Logical Frameworks and Meta-Languages: Theory and Practice, 9 September, Copenhagen, Denmark; LAM 2012: Fifth International Workshop on Logics, Agents, and Mobility, June, Hamburg, Germany; LPAR-18: The 18th International Conference on Logic for Programming, Artificial Intelligence and Reasoning. Merida, Venezuela, 11-15 March.

Dale Miller organized the Special Session on Structural Proof Theory and Computing at the 2012 Annual Meeting of the Association of Symbolic Logic (ASL), Madison, Wisconsin, 31 March - 3 April.

Kaustuv Chaudhuri and Stefan Hetzl organized the Collegium Logicum 2012 workshop at Inria Saclay during 15–16 November

Kaustuv Chaudhuri and Brigitte Pientka organized the RAPT/PROMIS workshop in Montreal, Canada, during 14–18 October

8.1.2. Invited Talks

Dale Miller gave an invited talk at the Journees nationales du GDR-IM, 25-26 January 2012, University of Paris 7.

Dale Miller gave an invited talk at the ANR-DFG Hypothese Workshop titled Different Aspects of Proof Theory, ENS Paris, 3 May 2012.

Dale Miller gave research talks at the following venues: Summer Workshop on Proof Theory, Pisa, Italy, 12-15 June; CHocCoLa seminar, ENS Lyon, 15 March; Workshop on Certificates and Computation, ITU Copenhagen, 12 March; Department of Mathematics, Carnegie Mellon University, 5 April.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence : Stéphane Graham-Lengrand teaches 50 hours (eq. TD) in L3 at Ecole Polytechnique in the course "INF431: Algorithmique et programmation".

Master : Dale Miller taught 12 hours at MPRI (Master Parisien de Recherche en Informatique) in the Course 2-1: Logique linéaire et paradigmes logiques du calcul.

Master : Stéphane Graham-Lengrand teaches 36 hours (eq. TD) in M1 at Ecole Polytechnique in the course "INF551: Computer-aided reasoning", and 15 hours (eq. TD) in M2 at Master Parisien de Recherche en Informatique (MPRI) on "Curry-howard correspondence for classical logic".

8.2.2. Supervision

PhD in progress :

1. Zakaria Chihani, since October 2012, supervisor: Dale Miller
2. Mahfuza Farooque, since October 2010, co-supervisor: Stéphane Graham-Lengrand
3. Ivan Gazeau, since October 2009, co-supervisor: Dale Miller
4. Nicolas Guenot, since October 2008, supervisor: Lutz Straßburger
5. Hernán-Pablo Vanzetto, since October 2010, co-supervisor: Kaustuv Chaudhuri

8.2.3. Juries

Dale Miller served as a reporter for the habilitation of Stefan Hetzl (Fall 2012) and was the president of the jury for the habilitation of Frédéric Blanqui, 13 July 2012.

Dale Miller served as a member of the PhD jury for Robert Simmons, Carnegie Mellon University, 22 October 2012. He was also "rapporteur" for the PhD of Nicolas Pouillard, University of Paris 7, 13 January 2012.

PI.R2 Project-Team

8. Dissemination

8.1. Scientific Animation

8.1.1. *Collective responsibilities*

Hugo Herbelin coordinated the ADT Coq and the development of Coq.

8.1.2. *Editorial activities*

Pierre-Louis Curien is co-editor in chief of Mathematical Structures in Computer Science, and is an editor of Higher-Order and Symbolic Computation.

8.1.3. *Program committees and organising committees*

Pierre-Louis Curien was member of the PC for ICALP 2012.

Pierre-Louis Curien, Yves Guiraud, Philippe Malbos and Alexis Saurin have been members of the organising and scientific committee of the Logic and Interactions weeks held in the CIRM, Marseille, in the first trimester of 2012.

Yann Régis-Gianas served on the PC for the conference "Journees Francophones des Langages Applicatifs" (2013).

Hugo Herbelin was in the PC of the conference ITP 2012 and MFCS 2012. He was in the PC of the TYPES 2011 conference post-proceedings.

Hugo Herbelin organised the "Automation in Proof Assistant" satellite workshop of ETAPS 2012 which was shared with the organisation of the first COST 0901 meeting of year 2012.

Matthieu Sozeau was in the PC of the MSFP'12 (colocated with ETAPS'12) and LFMTP'12 (colocated with ICFP'12) workshops. He was in the PC of the PLPV'12 workshop, colocated with POPL'12, for which he was an external reviewer as well. Matthieu Sozeau is in the PC of JFLA'13.

8.1.4. *Jury participation*

In June and July 2012, Alexis Saurin has been member of the Jury for entrance exams at ENS Paris and examined the candidates for the three ENS for the "Informatique Fondamentale" Oral exam.

In September 2012, Alexis Saurin has been member of the Jury for LMFI Master.

8.1.5. *Invited talks*

Matthieu Sozeau gave an invited lecture on type classes at JFLA'12 in Carnac (January 2012) and at U. Penn, in October 2012.

Pierre-Louis Curien was invited speaker at the annual meeting of the GDR Topologie et Applications, Lille ("Interprétation catégorique de la théorie des types : questions de cohérence"), in October 2012.

Pierre Letouzey gave an invited talk in the ML workshop in Copenhagen in September 2012, about the interactions between Coq and OCaml.

Alexis Saurin gave an invited talk at the ASL annual meeting held in Madison, Wisconsin, in April 2012 (special session on Structural Proof Theory and Computing).

8.1.6. *Presentation of papers*

Matthias Puech has presented his paper [25] at the TLDI 2012 workshop.

Yann Régis-Gianas has presented the paper [21] at the MIPS 2012 workshop (best paper award).

Pierre Boutillier has presented his paper at JFLA 2012.

Hugo Herbelin and Matthieu Sozeau have presented their papers at LICS 2012 in Dubrovnik, Croatia.

Hugo Herbelin has presented his joint paper with Zena Ariola, Paul Downen, Keiko Nakata and Alexis Saurin at FLOPS 2012 in Kobe, Japan.

8.1.7. *Other presentations*

Pierre Boutillier gave a talk at Logic and Interaction weeks in February.

Pierre Boutillier gave a talk about compiling Agda style dependent pattern-matching in CIC during AIPA workshop in Tallinn.

Jaime Gaspar gave talks at Colloquium Logicum 2012, Paderborn, in September, and Collegium Logicum 2012: Structural Proof Theory, at École Polytechnique, in November.

Tim Griffin gave the following presentations: "Mathematics of Inter-domain routing", at Internet Engineering Task Force (IETF), Paris, March; "Routing in Equilibrium" for the "Paris Networking Group" (http://www.paris-networking.org/display_event.php?dispID=2221), Paris, and at Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (ALGOTEL) (http://algotel2012.ens-lyon.fr), Montpellier.

Hugo Herbelin gave a talk on his proof-as-program interpretation of dependent choice in classical logic to the Réalisabilité à Chambéry #5 workshop in June.

Hugo Herbelin gave a talk on his proof with side-effects of Gödel's completeness theorem to the Workshop on Formal and Automated Theorem Proving and Applications (FATPA'12) held at the university of Belgrade.

Pierre-Marie Pédrot gave a presentation at the Logic and Interactions weeks in February, entitled "Double-glueing and orthogonality: refining models of linear logic through realizability".

8.1.8. *Talks in seminars*

Nicolas Ayache gave a talk about the achievements of the CerCo project at the seminar of the ENSTA, at the seminar of the EPITA and at the "GT programmation".

Pierre-Louis Curien gave a talk "De la logique classique (polarisée) à la logique linéaire (tensorielle)" at the Groupe de Travail Sémantique des calculs classiques, PPS, Paris 7, in November.

Pierre-Louis Curien gave talks on "System L syntax for sequent calculi" at the University of Bath, in February, at the École Polytechnique, in May, and at the Institute of Cybernetics, Tallinn, in December.

Jaime Gaspar gave talks at the Seminar of the Deducteam team, and at the Mathematical Logic Seminar, Lisbon.

Tim Griffin gave the following talks: "Routing in Equilibrium", University of Rome-3, April; "Routing in Equilibrium with help from ssreflect", Marelle team at École Polytechnique, May; "Mathematics of Routing", DIMACS working group on Abstractions for Network Services, Rutgers University, New Jersey, in May; "Mathematics of Routing", Université d'Évry, in June.

Yves Guiraud gave two talks on "Théorie de Squier et résolutions polygraphiques" at the Groupe de Travail Catégories supérieures, polygraphes et homotopie, PPS, Paris 7, in June.

Hugo Herbelin gave a talk on the formalisation of semi-simplicial sets in type theory at the Univalent Foundations seminar of the Institute for Advanced Study, Princeton, NJ, in December.

Guillaume Munch-Maccagnoni gave a talk about "Runnable monads in models of the λ calculus" at the ANR Logoi meeting in Luminy, in June.

Guillaume Munch-Maccagnoni gave a talk "On the computational contents of an involutive negation" at the Groupe de Travail Sémantique des calculs classiques, PPS, Paris 7, in November.

Pierre-Marie Pédrot gave a talk on a "Dependent delimited control monad" at the working group of the "Logique de la Programmation" team, from Institut Mathématique de Luminy, in December.

Matthieu Sozeau gave a talk in Tallinn about "Equations: A Dependent Pattern-Matching Suite" in June 2012.

Matthieu Sozeau gave a talk and a tutorial on "Coq with Classes" at the Institute for Advanced Study, Princeton, NJ in October and December 2012.

Matthieu Sozeau gave a talk about "Universe Polymorphism and Inference in Coq" at the Institute for Advanced Study, Princeton, NJ in December 2012.

8.1.9. *Attendance to conferences, workshops, schools,...*

Pierre Boutillier attended the Journées Francophones des Langages Applicatifs, Carnac, in February.

Tim Griffin attended the ssreflect/Inria MAP Spring School, Sophia Antipolis, in March.

Hugo Herbelin attended the FATPA workshop at the University of Belgrade in January.

Hugo Herbelin attended the ETAPS 2012 conference and the AIPA workshop in Tallinn in March-April.

Hugo Herbelin attended the FLOPS 2012 conference in Kobe in May.

Hugo Herbelin attended the ITP 2012 conference at Princeton University in August.

Hugo Herbelin attended the Coq workshop 2012 at Princeton University in August.

Guillaume Munch-Maccagnoni attended APLAS, Kyoto, in December.

Matthias Puech attended POPL 2012 in January.

Yann Régis-Gianas attended FMICS 2012, Paris, in August.

Matthieu Sozeau attended the POPL 2012 conference in January.

Matthieu Sozeau attended the JFLA 2012 conference in February.

8.1.10. *Groupe de travail Théorie des types et réalisabilité*

This is one of the working groups of PPS, jointly organised by Hugo Herbelin and Paul-André Melliès, since September 2009. It is held weekly. Yves Guiraud took over from Hugo Herbelin for the organisation of the seminar while Hugo was at IAS (October-December).

The web site is http://www.pps.univ-paris-diderot.fr/gdt-types-realisabilite. The programme in 2012 included talks by Pierre-Louis Curien, Arnaud Spiwack, Hugo Herbelin, Matthias Puech, Pierre Boutillier (twice), Federico Aschieri, Jaime Gaspar, Pierre-Marie Pédrot, François Bobot.

8.2. Teaching - Supervision - Jury participation

8.2.1. *Teaching*

(We do not include here the standard teaching duties of Pierre Letouzey and Yann Régis-Gianas as "Maîtres de conférences".)

Licence: Pierre Boutillier is teaching assistant at University Paris 7. He taught this year Unix-system (beginner), algorithms and databases (beginner in the bioinformatics master).

Licence: Matthias Puech has a temporary research and teaching position (A.T.E.R) at University Paris 7 for the academic year 2012–2013. He teaches this year logic (L2) and functional programming (L3) and abstract machines (L3).

Master: Yann Régis-Gianas took part in the MPRI course entitled "Type systems": he gave a 12 hours course about generalised algebraic data types, higher-order Hoare logic and dependently typed programming.

Master: Alexis Saurin taught the LMFI course entitled "Lambda-calcul et preuves" together with Thomas Ehrhard (January-May). Each of them taught half of this 48H master course.

Master: Pierre-Louis Curien gave a 10 hours course at the Department of Computer Science of the University of Oregon on proof theory (May).

Doctorat: Pierre-Louis Curien gave lectures at the 11th Oregon Summer School on Programming Languages (July).

Training: Pierre Letouzey participated to a training program for high-school teachers, introducing them to computer science. These teachers are meant to participate later to the new "Spécialité" ISN (Informatique et Sciences du Numérique) in "Terminale" grade.

8.2.2. Supervision

Internship: Yann Régis-Gianas supervised the internship of François Ripault.

Internship: Yann Régis-Gianas supervised the internship of Arthur Guillon.

PhD: Matthias Puech, Certificates for incremental type checking, Università di Bologna et Université Paris 7, December 2012, Hugo Herbelin, Andrea Asperti, and Yann-Régis Gianas.

PhD in progress: Pierre Boutillier, Représentation des effets et inférence de type dans le cadre du développement d'un langage de programmation à types riches, September 2010, Hugo Herbelin.

PhD in progress: Lourdes del Carmen Gonzalez Huesca, Un langage de tactiques typées pour Coq, December 2011, Hugo Herbelin and Yann-Régis Gianas.

PhD in progress: Guillaume Munch-Maccagnoni, Polarités, réalisabilité classique, contrôle délimité, September 2009, Pierre-Louis Curien and Thomas Ehrhard.

PhD in progress: Pierre-Marie Pédrot, Types dépendants et linéarité, October 2012, Hugo Herbelin and Alexis Saurin.

PhD in progress: Guillaume Claret, October 2012, Yann Régis Gianas.

8.2.3. PhD or habilitation jury participation

Pierre-Louis Curien was a referee for the PhD theses of Martin Churchill ("Imperative programs as proofs via game semantics", Univ. of Bath), Benedikt Ahrens ("Initiality for typed syntax and semantics", Université Nice Sophia Antipolis), Silvia Vecchiato ("Semantics of CBN dual proofs into control categories", Università di Siena), and Thomas Seiller ("Logique dans le facteur hyperfini: Géométrie de l'interaction et complexité", Université Aix-Marseille). He was member of the habilitation jury of Micaela Mayero ("Problèmes critiques et preuves formelles", Université Paris 13).

8.3. Popularisation

Yann Régis-Gianas organised the "Fête de la Science" event for the computer science department of the University Paris 7. François Bobot, Guillaume Claret, Lourdes Gonzalez-Huesca and Pierre-Marie Pédrot also took part in the animation.

Yann Régis-Gianas co-organised the "Journée Francilienne de Programmation", a programming contest between undergraduate students of three universities of Paris (UPD, UPMC, UPS).

Yann Régis-Gianas co-organised the "Robocup", a robotic and programming contest between undergraduate students of three universities of Paris (UPD, UP13, UP5).

Pierre Letouzey and Pierre Boutillier took part in the animation of the "Fête de la science" event at Inria Rocquencourt.

Yann Régis-Gianas gave one of the lectures to high-school teachers of the Académie de Paris in the context of the new curriculum "Informatique et Science du Numérique" (ISN).

PROSECCO Project-Team

9. Dissemination

9.1. Editorial Boards

- *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers, Associate Editor: Bruno Blanchet

9.2. Organizers

- Dagstuhl Analysis of Security APIs, November: Graham Steel
- ASA-6, Satellite of CSF, June: Graham Steel

9.3. Program Committees

- FCC – June 2012, Cambridge, MA, USA: Bruno Blanchet
- FM – August 2012, Paris, France: Bruno Blanchet
- CCS – October 2012, Ralleigh, NC, USA: Bruno Blanchet
- POST – March 2013, Rome, Italy: Bruno Blanchet
- PROOFS workshop - September 2012, September 2012: Graham Steel
- ACM SAC - Security Track 2012: Graham Steel

9.4. Vulnerability Reports

- R. Bardou and G. Steel (and their co-authors) found a series of vulnerabilities in cryptographic devices, resulting in a research paper and significant press coverage.
- K. Bhargavan and C. Bansal reported single sign-on vulnerabilities in Facebook, Yahoo, Helios and ConfiChair. These vulnerabilities were fixed on their recommendations, and the Prosecco team name was given credit on their websites.
- K. Bhargavan and A. Delignat-Lavaud reported encryption-related vulnerabilities in several commercial software packages, including 1Password, Roboform, LastPass, SpiderOak, and Wuala. These vulnerabilites were fixed on their recommendations and the Prosecco team was given credit on their websites.
- K. Bhargavan reported a CSP-related security vulnerability in Firefox, resulting in a security update.
- A. Delignat Lavaud reported a iframes-related security vulnerability in Firefox, resulting in a security update.

9.5. Teaching

- Karthikeyan Bhargavan taught TDs in computer science at Ecole Polytechnique, France
- Graham Steel taught invited Master's lectures at University of Venice, Italy
- Bruno Blanchet taught Master's lectures at the MPRI, France

9.6. Ph.D in progress

- David Cadé
  Computationally Proved Implementations of Security Protocols,
  since September 2009, supervised by Bruno Blanchet

- Miriam Paiola
  Automatic Verification of Group Protocols,
  since November 2010, supervised by Bruno Blanchet

- Robert Künnemann, *Secure APIs and Simulation-Based Security*, Started Oct. 2010, supervised by Steve Kremer (CASSIS) and Graham Steel

- Gavin Keighren, *A Type System for Security APIs*, since 2007 (to submit March 2013), advisors Graham Steel and David Aspinall (University of Edinburgh). Graham is now at EPI Prosecco.

9.7. Ph.D/Habilitation Committees

- Vincent Cheval – Ph.D. – 3 Dec. 2012 – ENS Cachan
  Automatic verification of cryptographic protocols: privacy-type properties
  Bruno Blanchet

9.8. Invited Talks

- Workshop on Computed-Aided Security, Grenoble, France, January: Bruno Blanchet

- ETAPS unifying invited speaker, Tallinn, Estonia March: Bruno Blanchet

- Workshop on Formal and Computational Cryptographic Proofs, Cambridge, UK (April): Bruno Blanchet

- Alan Turing Year workshop: Is Cryptographic Theory Practically Relevant?, Cambridge, 31 January - 2 February: Graham Steel

- PROOFS workshop, satellite of CHES, September: Graham Steel

- DIGITEO Forum, Ecole polytechnqiue November: Graham Steel

- Ruhr University Bochum Seminar, June: Graham Steel

9.9. Participation to Workshops and Conferences

- Workshop on Computed-Aided Security – January 2012, Grenoble, France: Bruno Blanchet, David Cadé, Miriam Paiola

- CryptoForma – March 2012, UK: Alfredo Pironti

- ETAPS – March 2012, Tallinn, Estonia]: Bruno Blanchet, David Cadé, Miriam Paiola

- Workshop on Formal and Computational Cryptographic Proofs – April 2012, Cambridge, UK: Bruno Blanchet

- IEEE S&P – May 2012, San Francisco, USA: Graham Steel

- CSF, FCC, ASA – June 2012, Cambridge MA, USA: Bruno Blanchet, David Cadé, Miriam Paiola, Graham Steel, Robert Künnemann, Karthikeyan Bhargavan, Romain Bardou

- Usenix Security – August 2012, Bellevue WA, USA: Karthikeyan Bhargavan, Antoine Delignat-Lavaud

- ARES – August 2012, Prague, Czech Republic: David Cadé

- CRYPTO – August 2012, Santa Barbara, USA: Graham Steel, Romain Bardou

- PROOFS – September 2012, Leuven Belgium: Graham Steel, Evmorfia-Iro Bartzia, Miriam Paiola

- MSR-Inria Workshop – November 2012, Cambridge UK: Karthikeyan Bhargavan, Alfredo Pironti

SECSI Project-Team

8. Dissemination

8.1. Scientific Animation

Administrative charges:

- Hubert Comon-Lundh is director of the Parisian Master of Research in Computer Science (MPRI).
- Hubert Comon-Lundh is member of the "comité de pilotage", labex Digicosme.
- Hubert Comon-Lundh is member of the "commission formation", labex Digicosme.
- Hubert Comon-Lundh is member of the "Jury prix de these Gilles Kahn/SIF".
- Stéphanie Delaune is a member of the scientific committee of Inria Saclay since February 2012.
- Stéphanie Delaune is "Déléguée aux thèses" at the École Doctorale Sciences Pratiques at ENS Cachan since September 2012.
- Jean Goubault-Larrecq, in charge of computer science questions, common Ecole Polytechnique-ENS Paris, Lyon, Cachan-ESPCI entrance competitive exam, starting September 2012.

Editorial boards:

- Hubert Comon-Lundh is associate editor of the ACM Transactions on Computational Logic.
- Hubert Comon-Lundh is guest editor of the Journal of Automated Reasoning (special issue, security and rewriting, Feb 2012).

Participation to program committes of conferences:

- 16th International Conference on Foundations of Software Science and Computation Structures FoSSaCS'13, Rome, Italy, March 2013 (Jean Goubault-Larrecq).
- 27th Annual ACM/IEEE Symposium Logic in Computer Science, Dubrovnik, Croatia, 2012 (Hubert Comon-Lundh)
- 8th International Conference on Information Security Practice and Experience ISPEC'12, Hangzhou, China (Stéphanie Delaune).
- 24th *Journées Francophones des Langages Applicatifs* JFLA'13, Aussois, France, February 2013 (David Baelde).

Selection committees:

- Hubert Comon-Lundh was president of selection committee, MCF, ENS Cachan 2012.
- Hubert Comon-Lundh was president of the selection committee for the mixed chair CNRS-Aix Marseille University, 2012.

Evaluation committees:

- Hubert Comon-Lundh, member of the jury of "Prime d'Excellence Scientifique" (National committee, professors and maîtres de conférences), 2012.
- Jean Goubault-Larrecq, AERES evaluation, LIAFA, Université Paris Diderot, December 27-28, 2012
- Jean Goubault-Larrecq, CNRS PEPS program evaluation committee, March 22, 2012

Scientific boards:

- Hubert Comon-Lundh, CNRS INSII, Oct. 2010-Oct 2014
- Jean Goubault-Larrecq, external member of the selection committee of the Formal Methods and Security Inria-DGA seminar, Rennes

Invited talks:

- Hubert Comon-Lundh *Towards unconditional soundness*. Grenoble, Jan 13, 2012, Workshop on Computer-Aided Security.
- Jean Goubault-Larrecq, *Probability and Nondeterminism in Domain Theory, Part II*, Logic and Interactions, week 4: Quantitative approaches, Marseilles, France, February 20-24.

Invitation to seminars:

- Stéphanie Delaune, Dagstuhl seminar on Analysis of security APIs, Wadern, Germany, November 25-28.
- Stéphanie Delaune, *Analysing privacy-type properties using formal methods*, CAPPRIS meeting, Paris, March 14
- Jean Goubault-Larrecq, *An Isomorphism between Powercone and Prevision Models*, McGill seminar, Bellairs Institute, Holetown, Barbados, April 01-06.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Licence :

- Rémy Chrétien, *Initiation à l'informatique* (TP), 39h., L1, Université Paris 7, Paris, France
- Hubert Comon-Lundh *Logic and Computability*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Programming*, 42h., L3, ENS Cachan, France
- Jean Goubault-Larrecq, *Logic and Computer Science* (a.k.a., the lambda-calculus), 36h., L3, ENS Cachan and ENS Paris, France
- Jean Goubault-Larrecq, Internship reviews, 4h., L3, ENS Cachan, France
- David Baelde, *Logic and Computability*, 45h., L3, ENS Cachan, France
- David Baelde, Internship reviews, 3h., L3, ENS Cachan, France

Master :

- Jean Goubault-Larrecq, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 1/3, 4h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Stéphanie Delaune, *Cryptography, Cryptographic Protocols and Quantum Cryptography*, Part 2/3, 4h., M1, Séminaire Regards Croisés Mathématiques-Physique, ENS Cachan, France
- Jean Goubault-Larrecq, *Advanced Complexity*, 42h., M1, MPRI course 1-17, France
- Jean Goubault-Larrecq, Internship reviews, 4h., M1, ENS Cachan, France
- Hubert Comon-Lundh, Internship reviews, 32h, M2 MPRI
- Jean Goubault-Larrecq, Internship reviews, 16h., M2, MPRI, France
- Hubert Comon-Lundh *Computational Soundness*, 12h., M2, MPRI course 2-30, France, Jan-Feb 2012
- Hubert Comon-Lundh *Formal proofs of security*, 24h, M2, MPRI course 2-30, France Oct-Dec 2012 (48h)
- Hubert Comon-Lundh *Preparation option info agreg: logique*, 24h, préparation à l'agrégation de Mathématiques, Jan-May 2012, ENS Cachan, France
- Hubert Comon-Lundh, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France

- Jean Goubault-Larrecq, rehearsal of Computer Science Lessons, préparation à l'agrégation de Mathématiques, 18h., ENS Cachan, France

8.2.2. Supervision

PhD :

- Vincent Cheval, *Automatic verification of cryptographic protocols: privacy-type properties*, ENS Cachan, Dec. 03, 2012 [12], supervised by Stéphanie Delaune and Hubert Comon-Lundh
- Hedi Benzina, *Enforcing virtualized systems security*, ENS Cachan, Dec. 17, 2012 [11], supervised by Jean Goubault-Larrecq

PhD in progress :

- Rémy Chrétien, *Trace equivalence for an unbounded number of sessions*, Started Oct. 2012, supervised by Stéphanie Delaune
- Robert Künnemann, *Secure APIs and Simulation-Based Security*, Started Oct. 2010, supervised by Steve Kremer and Graham Steel; Graham and Robert are now at EPI Prosecco
- Gavin Keighren, *A Type System for Security APIs*, since 2007 (to submit March 2013), advisors Graham Steel and David Aspinall (University of Edinburgh). Graham is now at EPI Prosecco.
- Guillaume Scerri, *Preuves abstraites de protocoles cryptographiques concrets*, Started Oct. 2011, supervised by Hubert Comon-Lundh

Masters:

- Rémy Chrétien, *Trace equivalence of protocols for an unbounded number of sessions*, 2012, advisors Stéphanie Delaune and Véronique Cortier
- Apoorvaa Deshpande, *Automated verification of equivalence properties modulo AC*, 2012, advisors Stéphanie Delaune and Steve Kremer

8.2.3. Juries

- PhD:
  – Hubert Comon-Lundh, president of the jury: Jeremy Planul, *Typage, compilation, et cryptographie pour la programmation répartie securisée*, Ecole Polytechnique, Feb 08, 2012.
  – Hubert Comon-Lundh, member of the jury: Vincent Cheval, *Preuves automatiques d'indistinguabilité*, ENS Cachan, Dec 03, 2012.
  – Jean Goubault-Larrecq, member of the jury: Gabriel Kerneis, *Continuation-Passing C: Program Transformations for Compiling Concurrency in an Imperative Language*, Université Paris Diderot, November 09, 2012.
  – Jean Goubault-Larrecq, member of the jury: Hedi Benzina, *Enforcing virtualized systems security*, ENS Cachan, December 17, 2012

- HdR:
  – Hubert Comon-Lundh, reviewer of the habilitation and member of the jury: Karthikeyan Bhargavan, *Towards the Automated Verification of Cryptographic Protocol Implementations*, Ecole Normale Supérieure, May 04, 2012.
  – Hubert Comon-Lundh, reviewer of the habilitation and member of the jury: Pascal Lafourcade *Cryptographic Primitives, Voting protocols, and Wireless Sensor Networks*, Université Joseph Fourier, Grenoble, Nov. 06, 2012.
  – Hubert Comon-Lundh, president of the jury: Jérôme Leroux, *Machines à compteur et arithmétique de Presburger*, Université Bordeaux I, Bordeaux, Dec 06, 2012.

– Jean Goubault-Larrecq, member of the jury: Laurent Doyen, *Games and Automata: From Boolean to Quantitative Verification*, ENS Cachan, March 13, 2012

8.3. Popularization

- Hubert Comon-Lundh , *Le vote électronique*, Institut des Hautes études en Sciences et Technologies (IHEST), Jan 20, 2012

- Stéphanie Delaune, member of the scientific mediation committee at Inria Saclay. ("Mediation" is the new name for popularization.)

- Jean Goubault-Larrecq, *Sécurité informatique*, talk and discussion with the public at the "débat citoyen" organized by Inria, Alan Turing building, Inria Saclay, November 19, 2012

- Jean Goubault-Larrecq, breakfast with the press, organized by CNRS, on computer security, November 29, 2012

- Stéphanie Delaune gave two popularization talks, *Ces protocoles qui nous protègent*, at *Journée Régionale de l'APMEP - Haute-Normandie*, Rouen, April 18, and at *Journée de rentrée de l'ENS Cachan*, Cachan, September 7.

- Stéphanie Delaune was interviewed by a journalist in charge of a special issue on cryptography for the magazine "Cahiers Sciences et Vie".

- Rémy Chrétien, *Le vote électronique*, article for the ANAJ-IHEDN Cybersecurity newsletter, to be published.

TASC Project-Team

9. Dissemination

9.1. Scientific Animation

- Nicolas Beldiceanu:
    - Head of the Inria TASC team and LINATASC team.
    - Program co-chair of CPAIOR 2012.
    - Member of the program committee of ROADEF 2012.
    - Member of the program committee of CP 2012.
    - Co-chair of BPPC 2012.
    - Member of the program committee of ECAI 2012.
    - Member of the program committee of CPAIOR 2013.
    - Member of the program committee of CP 2013.
    - Reviewer for IJCAI 2013.
    - Reviewer in 2012 for the Constraints Journal.
    - Invited talk in August 2012 on the topic of *a model seeker* by the Department of Information Technology, Uppsala University, Sweden.
- Fréderic Benhamou:
    - Vice-President for Research of Nantes University, France.
- Gilles Chabert:
    - Reviewer for CPAIOR 2012.
    - Reviewer for ACM-SAC 2012.
    - Reviewer in 2012 for the Constraints Journal.
    - Reviewer in 2012 for the RAIRO Journal.
    - Invited by the department of mathematics of Uppsala University, Sweden in the context of the international workshop on interval analysis and set-membership methods.
- Sophie Demassey:
    - Member of the program committee of CPAIOR 2012.
- Jean-Guillaume Fages:
    - Reviewer in 2012 for the Constraints Journal.
    - Invited an Inria Rocquencourt by the constraint team for a seminar on *Using Graph Variables in Constraints Programming*.
- Narendra Jussien:
    - Head of the computer science department at EMN.
    - Conference and program co-chair of CPAIOR 2012.
    - Member of the program committee of CP 2012.
    - Member of the program committee of LION 7.
    - Member of the program committee of RIVF 2012.
    - Member of the program committee of ROADEF 2012.
    - Member of the program committee of ACM-SAC 2012.
    - Reviewer in 2012 for the AI Journal.

- – Reviewer in 2012 for the TPLP.
- – Reviewer in 2012 for the Constraints Journal.
- – Director of the series *Operations Research and Constraint Programming* from ISTE/Wiley.

- Xavier Lorca:
  - – Member of the program committee of JFPC 2012.
  - – Member of the program committee of JFPC 2013.
  - – Member of the program committee of IJCAI2013.
  - – Reviewer for CPAIOR 2012.
  - – Reviewer in 2012 for the Constraints Journal.
  - – Reviewer in 2012 for the RAIRO Journal.

- Florian Richoux:
  - – Organizer and member of the program committee of the session *Large Scale Parallelism* of LION 7.

- Thierry Petit:
  - – Co head of the LINA TASC team.
  - – Conference co-chair of CPAIOR 2012.
  - – Member of the program committee of CPAIOR 2012.
  - – Member of the program committee of Cocomile 2012.
  - – Reviewer in 2012 for CP 2012.
  - – Reviewer in 2012 for the Constraints Journal.
  - – Reviewer in 2012 for EJOR.
  - – Reviewer in 2012 for CPL.
  - – Member of the program committee of CP 2013.
  - – Invited talk on the topic of *constraints on sequences of variables, balancing and focus constraints* at the 8èmes Journèes Francophones de Programmation par Contraintes (JFPC 2012), Toulouse, France.

- Charlotte Truchet:
  - – Program Chair of JFPC 2013.
  - – Member of the program committee of ECAI 2012.
  - – Invited at the NII (National Institute for Informatics) and JFLI (Japanese-French LAboratory for Informatics) in Tokyo: work on *parallel constraint solving* with H. Hosobe at NII and with P. Codognet at JFLI.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master: N. Beldiceanu, Constraint (Master ORO), 26h, M2, Nantes University, France.

Master: N. Beldiceanu, Logic Programming, 32h, M2, Mines de Nantes, France.

Master: N. Beldiceanu, Gipad end project, 8h, M2, Mines de Nantes, France.

Licence: N. Beldiceanu, Imperative Programming, 12h, L3, Mines de Nantes, France.

Licence: G. Chabert, Variational calculus, 12h, L3, Mines de Nantes, France.

Licence: G. Chabert, Numerical methods, 21h, L3, Mines de Nantes, France.

Licence: G. Chabert, Simulation and parameter estimation, 18h, L3, Mines de Nantes, France.

Licence: G. Chabert, Numerical integration, 15h, L3, Mines de Nantes, France.

Master: G. Chabert, Non-linear programming, 20h, M2, Mines de Nantes, France.

Licence: J.-G. Fages, Graphs and Algorithms, 28h, L2, Mines de Nantes, France.

Master: J.-G. Fages, Constraints Programming, 12h, M2, Mines de Nantes, France.

Master: J.-G. Fages, Project, 20h, M2, Mines de Nantes, France.

Licence: J.-G. Fages, Imperative Programming, 4h, L1, Mines de Nantes, France.

Master: N. Jussien, Constraint, 12h, M2, Mines de Nantes, France.

Master: N. Jussien, Constraint, 3h, M1, Mines de Nantes, France.

Licence: N. Jussien, Discrete mathematics, 12h, L3, Mines de Nantes, France.

Licence: A. Letort, Project, 15h, L1, Mines de Nantes, France.

Licence: A. Letort, Operation Research, 15h, L3, Mines de Nantes, France.

Master: X. Lorca, Head of the major of the Master in Engineering, Computer Science for Decision Support, M2, 30h, Mines de Nantes, France.

Master: X. Lorca, Algorithms and Complexity, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Data Warehouse and Data Analysis, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Graph Theory, Algorithms, 20h, M1, Mines de Nantes, France.

Master: X. Lorca, Business Intelligence, 20h, M2, Mines de Nantes, France.

Master: X. Lorca, IT System and Software Development, 20h, M2, Mines de Nantes, France.

Master: X. Lorca, Implementation Project, 20h, M2, Mines de Nantes, France.

Master: T. Petit, Combinatorial Optimization GIPAD, 17.5h, M2, Mines de Nantes, France.

Master: T. Petit, GIPAD project, 25h, M2, Mines de Nantes, France.

Master: T. Petit, Internship of Mohamed Kebe, 25h, M2, University of Clermont, France.

Licence: T. Petit, Imperative Programming, 22.5h, L2, Mines de Nantes, France.

Licence: T. Petit, Object Programming, 9h, L2, Mines de Nantes, France.

Licence: T. Petit, Synthesis, 5h, L2, Mines de Nantes, France.

Licence: T. Petit, Programming project, 8h, L2, Mines de Nantes, France.

Licence: T. Petit, Data structures, 27.5h, L2, Mines de Nantes, France.

Licence: F. Richoux, Design Patterns in Object-Oriented Programming, 96h, L3, University of Nantes, France.

Licence: F. Richoux, Introduction to Computer Science, 36h, L1, University of Nantes, France.

Licence: C. Truchet, C2i, 64h, L1, University of Nantes, France.

Licence: C. Truchet, Algorithms and Programming, 140h, L1, University of Nantes, France.

Licence: C. Truchet, Web, 36h, L1, University of Nantes, France.

Master: C. Truchet, Computer sound design, 24h, M2, University of Nantes, France.

9.2.2. Supervision

PhD: Marie Pelleau, Abstract domains in constraint programming, Nantes University, November 29 2012, Charlotte Truchet, Fréderic Benhamou, Pascal van Hentenryck.

PhD: Alexis De Clerq, Cumulative scheduling with overloads: global constraints and decompositions, Nantes University, October 29 2012, Thierry Petit, Narendra Jussien, Nicolas Beldiceanu.

PhD: Aurélien Merel, Biobjective railway infrastructure capacity assessment by hybrid column generation, Nantes University, October 31 2012, Sophie Demassey, Xavier Gandibleux.

PhD in progress: Arnaud Letort, Scalable scheduling constraints, October 2010, Nicolas Beldiceanu.

PhD in progress: Bruno Belin, Interactive conception of sustainable urban environments with constraints, September 2011, Charlotte Truchet, Marc Christie, Fréderic Benhamou.

PhD in progress: Jean Guillaume Fages, Graph Theory in Constraint Programming, Theory and application to several graph covering problems, October 2011, Xavier Lorca, Nicolas Beldiceanu.

PhD in progress: Charles Prud'Homme, Constraint Propagation and search strategies Management in Modern Constraint Solvers, October 2011, Xavier Lorca, Narendra Jussien, Rémi Douence.

PhD in progress: Alban Derrien, Constraint propagation with limited time complexity, October 2012, Thierry Petit, Nicolas Beldiceanu.

9.2.3. Juries

- N. Beldiceanu, Member of the PhD committee of the thesis of Alexis De Clerq (Univ. Nantes, October 29, 2012).
- F. Benhamou, Member of the PhD committee of the thesis of Marie Pelleau (Univ. Nantes, November 29, 2012).
- Narendra Jussien, Member of the PhD committee of the thesis of Alexis De Clerq (Univ. Nantes, October 29, 2012).
- Narendra Jussien, Reviewer of the PhD thesis of Caroline Maillet (Univ. Toulouse, April 25, 2012).
- T. Petit, Member of the PhD committee of the thesis of Alexis De Clerq (Univ. Nantes, October 29, 2012).
- Charlotte Truchet, Member of the PhD committee of the thesis of Marie Pelleau (Univ. Nantes, November 29, 2012).

9.3. Popularization

- Within the context of the global constraint catalog, some effort was done to provide more explanations for the core global constraints, namely:
  - provide for all core global constraints some small examples where one can see, also graphically, all solutions.
  - provide a set of 30 exercises with their detailed solution for half of the core constraints (*alldifferent*, *cycle*, *cumulative*, *element*, *nvalue*).
- Within the context of the new release of the library IBEX a course was given by G. Chabert mid december to about 22 participants in ENSTA Bretagne.

TOCCATA Team

9. Dissemination

9.1. Scientific Animation

9.1.1. Event organization

- C. Paulin organizer of the first DigiCosme Colloquium (http://labex-digicosme.fr/Colloque2012), Sept. 12-13, École Polytechnique, France.
- C. Paulin organizer of the 4th Conference on Interactive Theorem Proving (http://itp2013.inria.fr/) that will happen in July 2013.
- C. Marché organizer of the first DigiCosme Spring School (http://labex-digicosme.fr/Spring+School+2013 whose theme is *Program Analysis and Verification* and will happen in April 2013.

9.1.2. Editorial boards

- S. Boldo is member of the editorial committee of the popular science web site *interstices*, http://interstices.info/.
- J.-C. Filliâtre is member of the editorial board of the *Journal of Functional Programming*.
- C. Paulin is member of the editorial board of the *Journal of Formalized Reasoning*.

9.1.3. Learned societies

- J.-C. Filliâtre is a member of IFIP Working Group 1.9/2.15 (Verified Software)

9.1.4. Program committees

- C. Marché, *Tool Chair* of the program committee of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2013, Rome, Italy, http://www.etaps.org/2013/tacas13), part of the ETAPS joint Conference. The tool chair is responsible for the evaluation and selection of tool papers and tool demonstrations, following precise guidelines given in the call for papers. This initiative of TACAS aims at making the selection of such submissions more accurate (http://www.etaps.org/2013/tacas13/tacas13-tool-papers-menu).
- S. Conchon, member of the program committee of the 10th International SMT workshop 2012, Manchester, UK.
- C. Paulin, member of the program committee of the third and forth conferences on Interactive Theorem Proving (ITP 2012 & 2013 http://itp2013.inria.fr/).
- É. Contejean is a member of the program committees of the 23rd International Conference on "Rewriting Techniques and Applications" (RTA 2012 http://rta2012.trs.cm.is.nagoya-u.ac.jp/) and of the 24th International "Conference on Automated Deduction" (CADE-24 http://www.cade-24.info/).
- J.-C. Filliâtre is a member of the program committees of the second conference on Interactive Theorem Proving (ITP 2011), the workshop "Analyze to Compile, Compile to Analyze" (ACCA 2011), the conference Verified Software: Theories, Tools and Experiments (VSTTE 2012), the conference NASA Formal Methods (NFM 2012), and the 10th Asian Symposium on Programming Languages and Systems (APLAS 2012).

9.1.5. Invited Presentations

- S. Boldo, "Preuve de programmes d'analyse numérique", seminar of the AriC team, Lyon, January 5th.

- C. Lelay, "Improving Real Analysis in Coq: a User-Friendly Approach to Integrals and Derivatives", Coqapprox seminar (for the Tamadi ANR), Lyon, July 11th.
- C. Lelay, "Improving Real Analysis in Coq: a User-Friendly Approach to Integrals and Derivatives", LAC/LaMHA/LTP Days, Orléans, October 25th.
- G. Melquiond, "Wave Equation Numerical Resolution: a Comprehensive Mechanized Proof of a C Program", CaCoS Workshop, Grenoble, July 26th.
- J.-C. Filliâtre, "Combining Interactive and Automated Theorem Proving in Why3", Automation in Proof Assistants 2012, Tallinn, Estonia, April 2012.
- J.-C. Filliâtre, "Combining Interactive and Automated Theorem Proving using Why3 (invited tutorial)", Second International Workshop on Intermediate Verification Languages (BOOGIE 2012),Berkeley, California, USA, July 2012.

9.2. Interaction with the scientific community

9.2.1. Collective responsibilities within Inria

- S. Boldo, elected member of the Inria Evaluation Committee. She was in the committee in charge of selecting the Inria permanent researchers (CR2 and CR1).
- S. Boldo was in the committee in charge of selecting an Inria support staff (TR, *technicien de recherche*) for the Saclay finance and accounting service (SAF).
- S. Boldo, member of the CLHS, *comité local hygiène et sécurité* and member of the CLFP, *comité local de formation permanente*.
- S. Boldo, member of the committee for the monitoring of PhD students (*commission de suivi des doctorants*).
- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.
- S. Boldo, member of the popularization committee, *comité de médiation scientifique*, of Inria.
- C. Paulin was a member of the "Commission Scientifique" (in charge of selecting PhD students, post-doc, invited researchers funded by Inria Saclay - Île-de-France) until Aug.

9.2.2. Collective responsibilities outside Inria

- A. Charguéraud is vice-president of "France-IOI", the organization in charge of the selection and the training of the French team to the International Olympiads in Informatics.
- É. Contejean and C. Marché, nominated members of the *"conseil du laboratoire"* of LRI since April 2010.
- É. Contejean, elected member of the *"Section 6 du Comité National de la Recherche Scientifique"* since September 2012.
- S. Conchon, elected member of the *"Conseil scientifique de l'Université Paris-Sud"* since June 2012.
- C. Lelay, elected member of the *"conseil du laboratoire"* of LRI since November 2011.
- C. Lelay, elected representative of the students at the Doctoral School in Computer Science at University Paris-Sud since November 2011.
- C. Marché (since April 2007) and C. Paulin (since Sep. 2010), members of the program committee of Digiteo Labs, the world-class research park in *Île-de-France* region dedicated to information and communication science and technology, http://www.digiteo.fr/.
- C. Marché and S. Boldo, members of the *"jury de l'agrégation externe de mathématiques"* as experts in computer science, since 2012.

- G. Melquiond and C. Paulin, members of the *"commission consultative de spécialistes de l'université"*, Section 27, University Paris-Sud since April 2010.
- G. Melquiond, elected officer of the IEEE-1788 standardization committee on interval arithmetic since 2008.
- G. Melquiond is an examiner for the computer science entrance exam to École Normale Supérieure since 2010.
- C. Paulin, head of the new *Digicosme* laboratory of excellence (http://labex-digicosme.fr/)
- C. Paulin, director of the Doctoral school in Computer Science at University Paris-Sud http://edips.lri.fr/, until August 2012. Now in charge of the assembly of directors of graduate schools at the Université Paris-Sud.
- C. Paulin, member of the board of the "Commission Académique Consultative" of the Initiative d'Excellence Paris-Saclay.
- C. Paulin, president of the Computer Science Department of the University Paris-Sud https://www.dep-informatique.u-psud.fr/, since February 2012.
- C. Paulin participated to the hiring committee for a senior lecturer position at in Logic of Programs at University of Göteborg in Sweden.
- C. Paulin participated to two hiring commitees in France (professor positions at Paris-Sud University and CNAM)
- J.-C. Filliâtre is *correcteur au concours d'entrée à l'École Polytechnique* (computer science examiner for the entrance exam at École Polytechnique) since 2008.
- A. Paskevich is in charge (together with C. Bastoul) of Licence professionnelle PER (L3) at IUT d'Orsay, Paris-Sud University since September 2012.

9.3. Teaching - Supervision - Juries

9.3.1. Teaching

Master Parisien de Recherche en Informatique (MPRI) http://mpri.master.univ-paris7.fr/: "Proofs of Programs" http://www.lri.fr/~marche/MPRI-2-36-1/ (M2), C. Marché (12h), G. Melquiond (12h), Université Paris 7, France

Master Parisien de Recherche en Informatique (MPRI) http://mpri.master.univ-paris7.fr/: "Automated Deduction" https://wikimpri.dptinfo.ens-cachan.fr/doku.php?id=cours:c-2-5 (M2), S. Conchon (9h), É. Contejean (10h30), Université Paris 7, France

GDR Informatique-Mathématique school for young researchers: "Arithmétique des ordinateurs et preuves formelles" [35], S. Boldo (2h), G. Melquiond (2h).

C. Paulin lecture notes on "Introduction to the *Coq* proof-assistant for practical software verification" at the LASER 2011 Summer School on Software Engineering have been published [37].

École Jeunes Chercheurs en Programmation (EJCP 2012): J.-C. Filliâtre ,"Vérification Déductive de Programmes avec Why3" (4h) [36].

Licence (DUT): "Mathématiques" (L1), "Algo Langages" (L1), C. Lelay (64h, "moniteur" position), Université Paris-Sud (IUT d'Orsay)

Licence (L2): "Mathématiques pour l'Informatique" , C. Paulin (40h), D. Cousineau (20h), Université Paris-Sud

Licence (L3): "Eléments de logique pour l'informatique", C. Paulin (50h), Université Paris-Sud, France

Licence (L3): "Programmation fonctionnelle", S. Conchon (25h), A. Tafat (50h), M. Iguernelala (50h), Université Paris-Sud, France

Licence (L3): "Projet de programmation", S. Conchon (25h), Université Paris-Sud, France

Master (M1): "Projet de compilation" A. Tafat (33h), M. Iguernelala (33h), Université Paris-Sud, France

Master (M1): "Introduction à la compilation", S. Conchon (50h), Université Paris-Sud, France

Licence: "Langages de programmation et compilation" (L3), J.-C. Filliâtre (36h), École Normale Supérieure, France

Licence (DUT): "Systèmes d'exploitation" (L1 and L2), "Réseaux" (L2), A. Paskevich (140h), Université Paris-Sud (IUT d'Orsay), France

Licence professionnelle: "Programmation concurrente" (L3), A. Paskevich (36h), Université Paris-Sud (IUT d'Orsay), France

Licence: "INF421" (L3) et "INF431" (L3), J.-C. Filliâtre (70h), École Polytechnique, France

Master (M1): "Compilation", C. Dross, Université Paris-Sud (PolyTech)

9.3.2. Supervision of internships

J.-C. Filliâtre supervised the L3 internship of Rémy El Sibaïe on "Une bibliothèque OCaml pour la combinatoire" (May–June 2012) [85].

J.-C. Filliâtre supervised the M1 internship of Levs Gondelmans on "A Simple Induction Tactic for the Why3 Platform" (April–August 2012).

C. Paulin supervised the M2 internship of Nicolas Lupinski on "formalisation and proofs of program transformations for automated parallelisation".

9.3.3. Supervision of Theses

PhD: T. Nguyen, Taking architecture and compiler into account in formal proofs of numerical programs [12], Université Paris-Sud, June 2012, S. Boldo, C. Marché

PhD in progress: M. Iguernelala, Forward and Backward Strategies in SMT solvers, since September 2009, S. Conchon, É. Contejean

PhD in progress: A. Tafat, Modular Verification of Pointer Programs, since September 2009, C. Marché

PhD in progress: P. Herms, Certification of a Tool Chain for Verification of C programs, since October 2009, C. Marché, B. Monate (CEA List). Defence scheduled on January 14th, 2013.

PhD in progress: C. Dross, Theories and Techniques for Automated Proof of programs, since January 2011, C. Marché, A. Paskevich, and industrial supervisors Y. Moy and J. Kanig from AdaCore company.

PhD in progress: A. Mebsout, SMT-based Model-Checking, since September 2011, F. Zaidi, S. Conchon

PhD in progress: C. Lelay, Real numbers for the Coq proof assistant, since October 2011, S. Boldo, G. Melquiond.

PhD in progress: S. Dumbrava, Towards data certification, since October 2012, V. Benzaken, É. Contejean

9.3.4. Juries

- S. Boldo: PhD committee of Érik Martin-Dorel "Contributions to the Formal Verification of Arithmetic Algorithms" (ENS de Lyon, LIP laboratory, September 26th, 2012)

- C. Marché: reviewer, PhD committee of Morayo Adedjouma "Requirements Engineering Process according to Automotive Standards in a Model-Driven Framework" (University Paris-Sud, LISE laboratory of CEA-List, July 12th, 2012)

- C. Marché: president of the PhD committee of Florian Noyrit "Conception Dirigée par les modèles à l'aide de langages de modélisation hétérogènes : application aux profil UML" (University Paris-Sud, LISE laboratory of CEA-List, October 25th, 2012)

- C. Marché: president of the PhD committee of Takoua Ben Rhouma Aouina "Composition des modèles de lignes de produits logiciels" (University Paris-Sud, LISE laboratory of CEA-List, November 29th, 2012)

- C. Marché: president of the PhD committee of Abderrahmane Feliachi "Semantics Based Testing for Circus" (University Paris-Sud, LRI laboratory, December 12th, 2012)

- C. Marché: reviewer, Habilitation committee of Sylvie Putot "Static Analysis of Numerical Programs and Systems" (University Paris-Sud, MeASI laboratory of CEA-List and École Polytechnique, December 13th, 2012)

- C. Paulin: reviewer, PhD committee of Thomas Braibant, "Algèbres de Kleene, Automates, Circuits, Preuve formelle, Réecriture" (Université de Grenoble, Inria Rhone-Alpes, February 17th, 2012)

- C. Paulin: reviewer, PhD committee of Sylvain Héraud, "Vérification Semi-automatique de primitives cryptographiques" (Université de Nice Sophia-Antipolis, Inria Sophia Antipolis, March 12th, 2012)

- C. Paulin: president of the PhD committee of Stéphane Glondu "Vers une certification de l'extraction de Coq", (Université Paris Diderot, Laboratory PPS, June 1st, 2012)

- C. Paulin: reviewer, Habilitation committee of David Pichardie "Toward a Verified Software Toolchain for Java" (Université de Rennes, IRISA, November 19, 2012)

- C. Paulin: president of the PhD committee of Marc Lasson "Réalisabilité et Paramétricité dans les systèmes de type purs" (Université de Lyon, LIP Laboratory, November 20, 2012)

- J.-C Filliâtre: reviewer, PhD committee of Barbara Vieira, "Formal Verification of Cryptographic Software Implementations" (Universitad do Minho, Braga, Portugal, June 25, 2012).

- J.-C Filliâtre: Habilitation committee of Etienne Lozes, "Separation Logic: Expressiveness and Copyless Message-Passing" (ENS Cachan, July 3, 2012).

- J.-C Filliâtre: reviewer, PhD committee of Cyril Cohen, "Formalized algebraic numbers: construction and first order theory" (École Polytechnique, November 20, 2012).

- J.-C Filliâtre: reviewer, Habilitation committee of Frédéric Gava "BSP, bon à toutes les sauces" (Université Paris-est, December 10, 2012).

9.4. Industrial Dissemination

- J.-C. Filliâtre and C. Marché started in 2011 a collaboration with D. Mentré at Mitsubishi Electric R&D Centre Europe (Rennes), about the use of the *Why3* environment and its back-end provers as an alternative to the built-in prover of Atelier B. This collaboration leaded first to a publication [29] and then become part of the new ANR project BWare.

- Alt-Ergo is now used in the Spark Pro toolset, developed by Altran-Praxis, for the engineering of high-assurance software. Alt-Ergo can be used by customers as an alternate prover for automatically proving verification conditions. Its usage is described in the new edition of the Spark book (http://www.altranpraxis.com/book/, Chapter "Advanced proof tools")

- In the context of the Hi-Lite project, the Adacore company (Paris) implements a new tool GnatProve which aims at formal verification of Ada programs. They translate annotated Ada code into the *Why3* intermediate language and then use the *Why3* system to generate proof obligations and discharge them with Alt-Ergo, or other available back-end provers. GnatProve is a prototype that aims at becoming the successor of Spark (http://www.open-do.org/2012/11/30/future-version-of-spark-will-be-based-on-ada-2012/).

- S. Conchon, A. Mebsout and F. Zaidi (ForTesSe team, LRI) continued their collaboration with S. Krstic and A. Goel (Intel Strategic Cad Labs in Hillsboro, OR, USA) that aims in the development of the SMT-based model checker Cubicle (http://cubicle.lri.fr).

9.5. Popularization

- Since April 2008, S. Boldo is member of the editorial committee of the popular science web site)i(: http://interstices.info/.

- S. Boldo, scientific head for Saclay for the MECSI group for networking about computer science popularization inside Inria.

- S. Boldo, member of the popularization committee, *comité de médiation scientifique*, of Inria.

- S. Boldo visited two classes for the beginning of the computer science teaching in 2nde: lycée Jean Jaurès at Chatenay-Malabry and Jacques Monod at Clamart in January 2012.

- S. Boldo is responsible for a *mission doctorale* for popularization. She is in charge of Li Gong of the LIMSI laboratory.

- S. Boldo, head for the *Fête de la science* for the LRI laboratory in 2012. The laboratory welcomed both industrials, pupils and general public: 6 different stands, 6 classes, a total of more than 250 visiting persons.

- S. Boldo and A. Charguéraud belong to the organization committee of the *Castor informatique* http://castor-informatique.fr/, an international competition to present computer science to pupils (from *6ème* to *terminale*). More than 91,000 teenagers played on the 40 proposed exercises in November 2012.

- C. Lelay and A. Tafat are involved in the *Fête de la science* 2012.

TYPICAL Project-Team

8. Dissemination

8.1. Teaching - Supervision - Juries

8.1.1. Teaching

Benjamin Werner is president of the Computer Science Department of Ecole Polytechnique and, as such main responsible for CS teaching in this university.

Licence : Benjamin Werner, Ecole Polytechnique, *Algorithmique et Programmation*, lectures, 45 hours *équivalents TDs*.

Master : Benjamin Werner, MPRI (M2), Fondements des Systèmes de Preuves, Ecole Polytechnique et U. Paris 7, 50 heures équivalents TDs.

Master : Assia Mahboubi and Bruno Barras, MPRI (M2), Preuves en Coq, Ecole Polytechnique et U. Paris 7, 50 heures équivalents TDs.

Licence : Victor Magron and Chantal Keller, Ecole Polytechnique, *Algorithmique et Programmation*, TDs, 48 hours *équivalents TDs*.

Master : Chantal Keller, PA Informatique de l'Ecole Polytechnique, Raisonnement mathématique assisté par ordinateur, TDs, 20 hours *équivalents TDs*.

8.1.2. Supervision

PhD & HdR :

PhD : Cyril Cohen, Formalized algebraic numbers: construction and first-order theory, Ecole Polytechnique, november 20$^{\text{th}}$, Assia Mahboubi and Benjamin Werner.

PhD in progress :Chantal Keller, A Matter of Trust New Reflexive Decision Procedures in Coq Using External Tools, since sept. 2009, Benjamin Werner

PhD in progress :Victor Magron, Certifiable automatic proofs of real inequalities, since sept. 2009, Benjamin Werner and Stéphane Gaubert.

PhD in progress: Alexis Bernadet, since 2010. Supervised by Stéphane Lengrand and Benjamin Werner.

<div align="center">

VERIDIS Project-Team

</div>

9. Dissemination

9.1. Scientific Animation

- Pascal Fontaine co-chaired the program committee of PAAR 2012 and SMT 2012. He served on the program committee of PxTP 2012. He has been ex-officio member of the SMT Steering Committee starting September 2011 until August 2012, and he is now an elected member for two years starting September 2012.
- Dominique Méry is
  – a member of the IFIP Working Group 1.3 on *Foundations of System Specification*,
  – head of the Doctoral School IAEM Lorraine for the University of Lorraine,
  – head of the Formal Methods department of the LORIA laboratory,
  – an expert for the French Ministry of Education (DS9),
  – an expert for the French Agence Nationale de la Recherche (ANR) and AERES.
  – the director of international affairs at ESIAL Nancy, and
  – the president of the APCB association.
  – He served on the program committees of DS-Event-B, FHIES, FM (co-chair), ICECCS, ICFEM, iFM, MEDI, and TASE.
- The academic duties of Stephan Merz include:
  – member of the IFIP Working Group 2.2 on *Formal Description of Programming Concepts*,
  – nominated member of the Section 7 of the Comité National de la Recherche Scientifique (until the summer of 2012),
  – Inria representative in the Scientific Directorate of the International Computer Science Meeting Center in Dagstuhl,
  – delegate for the organization of conferences at Inria Nancy Grand-Est,
  – co-head of the PhD committee for computer science in Lorraine (since December 2012),
  – program committees of ICFEM, iFM, SAC, SBMF, and SEFM conferences, AVoCS (co-chair), ATX, and TLA (co-chair) workshops, steering committee of AVoCS,
  – co-organizer of the VTSA summer school between Nancy, Saarbrücken, Luxembourg, and Liège,
  – expert for the French Agence Nationale de la Recherche (ANR), AERES, German DFG, European ERC, and Canadian NSERC.

9.2. Teaching - Supervision - Juries

9.2.1. *Teaching*

The university employees of VeriDis have significant teaching obligations. We indicate the graduate courses they have been teaching this year, as well as significant pedagogical responsibilities.

- Dominique Méry gave courses in the Master program in Nancy on: formal system engineering, modeling and verification of systems, theoretical computer science, development of software systems, distributed algorithms.
- Stephan Merz taught a course on algorithmic verification in the Master program in Nancy (30 hours) and a course on modal logic in the undergraduate curriculum on cognitive and computer science (30 hours).

9.2.2. Supervision

PhD: Sabina Akhtar, Verification of Distributed Algorithms using PlusCal-2, Université de Lorraine, May 2012, supervised by Stephan Merz;

PhD in progress: Manamiary Andriamiarina, Refinement Techniques for Distributed Algorithms, since 10/2010, supervised by Dominique Méry;

PhD in progress: Henri Debrat, Formal Verification of Fault-Tolerant Distributed Algorithms, since 10/2009, supervised by Bernadette Charron-Bost and Stephan Merz;

PhD in progress: Tianxiang Lu, Verification of the Pastry Routing Protocol, since 05/2009, supervised by Stephan Merz and Christoph Weidenbach;

PhD in progress: Hernán Vanzetto, SMT Techniques for TLA$^+$ Proof Obligations, since 10/2010, supervised by Kaustuv Chaudhuri and Stephan Merz.

9.2.3. Juries

Dominique Méry wrote reports on the following PhD theses.

- Anton Tarasyuk: *Formal Development and Quantitative Verification of Dependable Systems*, University of Turku;

- Jean-Charles Chaudemar: *Etude des architectures de sécurité de systèmes autonomes – Formalisation et évaluation en Event B*, Université de Toulouse;

- Damien Imbs: *Calculabilité et conditions de progression des objets partagés en présence de défaillances*, Université de Rennes;

- Vincent Filou: *Une étude formelle de la théorie des calculs locaux à l'aide de l'assistant de preuve Coq*, Université de Bordeaux.

Stephan Merz wrote reports on the following PhD and habilitation theses:

- Francesco Bongiovanni: *Design, Formalization and implementation of overlay networks; application to RDF data storage*, Université de Nice-Sophia Antipolis;

- Abderrahmane Feliachi: *Semantics Based Testing for Circus*, Université Paris-Sud;

- Sylvain Conchon: *SMT Techniques and their Applications*, Université Paris-Sud.