# CURRICULUM VITÆ

2 NOVEMBRE 2017


## Jean-Guillaume Dumas

Professeur des universités en Mathématiques Appliquées (section 26)
à l'université Grenoble Alpes et au laboratoire Jean Kuntzmann, Grenoble.



**Animation scientifique** **2**
- Parcours professionnel et formation . . . 2
- Encadrement d'activités de recherche . . . 2
- Jurys de thèse et d'HDR . . . 3

**Activités d'enseignement** **5**
- Modules enseignés . . . 5
- Responsabilité de filière . . . 5
- Développement du Master 2 Cryptologie et Sécurité . . . 5
- Enseignement et recherche en cryptologie et codes . . . 6
- Développement à l'international . . . 6
- Écoles et enseignements de $3^{\text{ième}}$ cycle . . . 6

**Activités de recherche** **7**
- Calcul exact intensif . . . 7
  - Algèbre linéaire exacte. . . . 7
  - Conception et modélisation logicielles, algorithmique parallèle. . . . 7
  - Sécurité, cryptologie, codes, arithmétique. . . . 7
  - Algorithmes symboliques-numériques. . . . 8

**Rayonnement** **9**
- Activité éditoriales et de conseil scientifique . . . 9
- Comités de programmes et comités de lecture internationaux . . . 9
- Direction adjointe du Laboratoire Jean Kuntzmann . . . 10
- Responsabilité d'équipe de recherche . . . 10
- Commission de spécialistes et conseil d'UFR . . . 10
- Responsabilité des moyens informatiques . . . 10
- Prix, distinctions . . . 10
- Organisation de conférences . . . 10
- Communications, invitations et séjours de recherche internationaux . . . 11
- Communications, invitations et séminaires nationaux . . . 12

**Publications** **14**
- Publications de rang A . . . 14
- Publications de rang B . . . 18
- Monographies et chapitres de livres . . . 18
- Contrats de recherche . . . 19
- Logiciels (cf. http://ljk.imag.fr/CASYS/LOGICIELS) . . . 21
- Rapports de recherche et prépublications soumises . . . 21
- Co-auteurs . . . 21

**Références** **22**

# ANIMATION SCIENTIFIQUE

Jean-Guillaume Dumas, 42 ans, né le 13 février 1975 à Nice, nationalité française.


Université Grenoble Alpes
Laboratoire Jean Kuntzmann
Jean-Guillaume.Dumas@imag.fr
ljk.imag.fr/membres/Jean-Guillaume.Dumas

51, av. des Mathématiques,
BP 53X, 38041 Grenoble.
Tél. : 33 (0) 476 514 866
Fax. : 33 (0) 476 631 263


## Parcours professionnel et formation

Depuis 2016 : **Directeur du master**, CyberSecurity, UFR IM$^2$AG et Grenoble INP.

2014-2016 : **Directeur adjoint**, *laboratoire Jean Kuntzmann*, en charge du département MAD (modèles et algorithmes déterministes).

2013-2017 : **Vice chair** ACM SIGSAM (*Special Interest Group in Symbolic and Algebraic Manipulations*, élu).

2015-2017 : **Chair**, Steering committee, ACM PASCO conference series (*Parallel Symbolic Computation*).

Depuis 2012 : **Professeur des Universités**, section 26 mathématiques appliquées, à l'*université de Grenoble* et au *LJK*, Grenoble, France.

2012-2016 : **Coordinateur**, projet ANR HPAC (high-performance algebraic computing, Montpellier, Lyon, Paris, Grenoble).

2011-2015 : **Responsable du master 1**, mathématiques appliquées et industrielles, UFR IM$^2$AG.

Juillet 2010 : **Habilitation à diriger des recherches** de l'*Université de Grenoble* : contributions au calcul exact intensif.

2009-2010 : **Visiting Professor** à l'*University College Dublin*, School of Mathematical Sciences, Irlande, en délégation CNRS au *Claude Shannon Institute*, Dublin.

2002-2012 : **Maître de conférences**, section 26 Mathématiques appliquées, à l'*université Joseph Fourier* et au *laboratoire Jean Kuntzmann*, Grenoble, France.

2001-2002 : **ATER** à l'*ENSIMAG* et au *laboratoire de Modélisation et Calcul*, Grenoble : analyse qualitative des systèmes hybrides.

2000-2001 : **ATER** à l'*ENSIMAG* et au *laboratoire Informatique et Distribution*, Montbonnot Saint Martin : routines efficaces d'algèbre linéaire dense sur des corps finis.

1997-2000 : **Doctorat** de l'*INPG* au *laboratoire Informatique et Distribution* et à l'*université du Delaware*, USA : Algorithmes parallèles efficaces pour le calcul formel : algèbre linéaire creuse et extensions algébriques (mention très honorable avec félicitations du jury) ; **Monitorat** à l'université Joseph Fourier.

## Encadrement d'activités de recherche

### Thèses en cours

**2.** Thèse H2020-OPENDREAMKIT **David Lucas** (directeur C. Pernet) : *Robust and certified high performance algebraic computing*. Depuis octobre 2016.

**1.** Thèse PIA-ARAMIS **Jean-Baptiste Orfila** : *Architecture de sécurité et protocoles cryptographiques pour les systèmes de contrôle-commande*. Depuis octobre 2014.

### Thèses soutenues

**6.** Thèse ANR **Ziad Sultan**, projet ANR-11-BS02-013 HPAC (co-directeur C. Pernet) : *Parallel building blocks for high-performance algebraic computations*. Soutenue le 17 juin 2016. Z. Sultan est ensuite devenu ingénieur calcul haute-performance, Eolen Paris.

**5.** Thèse programme international **Burak Ekici** (co-directrice D. Duval) : *Certification de programmes avec des effets calculatoires*. Soutenue le 9 décembre 2015. B. Ekici est actuellement post-doctorant, U. Iowa.

4. Thèse MESR **Brice Boyer** : *Multiplication matricielle efficace et conception logicielle pour la bibliothèque de calcul exact* LinBox. Soutenue le 21 juin 2012.
3. Thèse MESR **Anna Urbańska** (directrice D. Duval) : *Hybrid and adaptive algorithms in exact linear algebra*. Soutenue le 27 avril 2010. Anna Urbańska est ensuite devenue en septembre 2010 **ingénieure R&D**, Google Zurich.
2. Thèse MESR **Clément Pernet** (directrice D. Duval) : *Algèbre linéaire exacte efficace : le calcul du polynôme caractéristique*. Soutenue le 27 septembre 2006. Clément Pernet est **maître de conférences** au laboratoire d'informatique de Grenoble et à l'université Joseph Fourier depuis septembre 2008.
1. Thèse MESR **Aude Rondepierre** (directeur J. Della Dora) : *Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires*. Soutenue le 18 juillet 2006. Aude Rondepierre est **maître de conférences** à l'INSA et à l'institut de mathématiques de Toulouse, depuis septembre 2008.

**Post-doctorants et ingénieurs de recherche**

4. Ingénieur de recherche projet OpenDreamKit **Zhu Hong Guang** : *Exact linear algebra routines over distributed memory plateforms and GPU*, 2017-2018.
3. Ingénieur de recherche projet Hpac **Alexis Breust** : *Routines d'algèbre linéaire exacte sur multicœurs*, 2014-2015.
2. Ingénieur de recherche projet MPLLC **Guillaume Ollier** : *Problèmes LWE et Ring-LWE : liens avec les réseaux, difficultés et implémentations pratiques*, 2011-2012.
1. Post-doctorat projet FUI-Shiva **Christophe Chabot** : *Entiers récursifs à précision fixée sur FPGA*, 2010-2011.

Direction de Master 2 Recherche : une (A. Rondepierre) en 2002, deux (C. Pernet et P. Vignard) en 2003, deux (J. Dubrois et I. Hatm) en 2004, un (B. Boyer) en 2008, un (A. Al Rashedi) en 2009, un (H. Hossayni) en 2011, un (JB Orfila) en 2014, un (V. Zucca) en 2015 et un (A. Bouguera) en 2016.

Participation à une vingtaine de jurys de DEA/M2R.

Direction d'une trentaine de TER Master 1 (en Informatique, en Mathématiques et en Mathématiques Appliquées à l'UJF et à l'ENSIMAG) : trois en 2003 ; quatre en 2004 ; deux en 2005 ; deux en 2006 ; sept en 2007 ; cinq en 2008 ; un en 2009 ; un en 2011 ; deux en 2012 ; cinq en 2013 ; un en 2014 ; un en 2015 ; deux en 2016 ; deux en 2017.

## Jurys de thèse et d'HDR

18. **Damien Jauvart** (rapporteur), U. Paris Saclay, *Sécurisation des algorithmes de couplage contre les attaques physiques*, septembre 2017.
17. **Mustafa Elsheikh** (rapporteur), U. of Waterloo, Canada, *Smith normal form of matrices over local rings*, août 2017.
16. **Chemseddine Chohra** (examinateur), U. de Perpignan via domitia, *Towards Reproducible, Accurately Rounded and Efficient BLAS*, mars 2017.
15. **Jon Haël Brenas** (président), U. Grenoble Alpes, *Hoare-like Verification of Graph Transformation*, octobre 2016.
14. **Ziad Sultan** (directeur), U. Grenoble Alpes, *Parallel building blocks for high-performance algebraic computations*, juin 2016.
13. **Christophe Negre** (habilitation, rapporteur), U. Montpellier, *Multiplication in finite fields and elliptic curves*, avril 2016.
12. **Mathilde Duclos** (président), U. Grenoble Alpes, *Méthodes pour la vérification des protocoles cryptographiques dans le modèle calculatoire*, janvier 2016.
11. **Burak Ekici** (directeur), U. Grenoble Alpes, décembre 2015.

10. **Clément Pernet** (habilitation, examinateur), U. de Grenoble, *Calcul algébrique haute performance fiable*, novembre 2014.
9. **Stef Graillat** (habilitation, examinateur), U. Pierre et Marie Curie (Paris 6), *Contribution à l'amélioration de la précision et à la validation des algorithmes numériques*, décembre 2013.
8. **Yanis Linge** (président), U. de Grenoble, *Etudes cryptographiques et statistiques de signaux compromettants*, novembre 2013.
7. **Bruno Grenet** (examinateur), ÉNS Lyon, *Représentations des polynômes, algorithmes et bornes inférieures*, novembre 2012.
6. **Brice Boyer** (directeur), U. de Grenoble, juin 2012.
5. **Thomas Izard** (rapporteur), U. de Montpellier, *Opérateurs parallèles pour la cryptographie asymétrique*, décembre 2011.
4. **Anna Urbańska** (co-directeur), U. de Grenoble, avril 2010.
3. **Clément Pernet** (co-directeur), U. J. Fourier, septembre 2006.
2. **Aude Rondepierre** (co-directeur), I. N. Polytechnique de Grenoble, juillet 2006.
1. **Éric Tannier** (examinateur), U. J. Fourier, *Sur quelques problèmes de recouvrement et empilement dans les graphes et les matroïdes*, septembre 2002.

# ACTIVITÉS D'ENSEIGNEMENT

Je suis professeur en section 26 du CNU. Mon enseignement au sein de l'université Grenoble Alpes se situe à l'interface Mathématiques et Informatique de la licence au master. Le tableau suivant résume les différents enseignements auxquels j'ai participé d'abord en tant que moniteur UJF, puis en tant qu'ATER Ensimag et enfin en tant que maître de conférences UJF puis professeur UGA.

## Modules enseignés

| Enseignement | Unité | Années | Niv. | Type | Nature | Eff. | Vol. |
|---|---|---|---|---|---|---|---|
| Security Architectures | UFR im$^2$ag | 2016- | M2 | FI | C/TD/TP | 20 | 60h |
| Introd. to cryptology and coding | MOSIG | 2015- | M1 | FI | C/TD/TP | 50 | 40h |
| Trait. algébrique de l'information | Ensimag | 2011- | M1 | FI | C/TD | 80 | 36h |
| Cryptographic engineering | UFR im$^2$ag | 2016- | M1 | FI | C/TD/TP | 25 | 40h |
| High-performance exact computing | UFR im$^2$ag | 2013-16 | M2 | FI | C | 10 | 18h |
| Sécurité Web | UFR im$^2$ag | 2011-16 | M2 | FI | C/TD | 12 | 36h |
| Architectures PKI | UFR im$^2$ag | 2010-16 | M2 | FI | C/TD/TP | 25 | 36h |
| Calcul exact | UFR im$^2$ag | 2005-09 | M2 | FI | C | 12 | 18h |
| Programmation Système | UFR im$^2$ag | 2010-15 | M1 | FI | C/TD/TP | 20 | 12h |
| C++ avancé | UFR im$^2$ag | 2010-15 | M1 | FI | Projets | 20 | 34h |
| Programmation efficace, jeux | UFR im$^2$ag | 2010-15 | M1 | FI | TP | 20 | 18h |
| Calcul formel et cryptographie | UFR im$^2$ag | 2010-16 | M1 | FI | C/TD/TP | 25 | 40h |
| Maths for fun | Ensimag | 2007-09 | M2 | FI | C | 40 | 18h |
| Information Algebraic Processing | MOSIG | 2006-07 | M1 | FI | C/TD | 25 | 24h |
| Réseaux, Internet, Sécurité | IUP MAI | 2003-04 | M1 | FI | C/TD/TP | 25 | 36h |
| Prog. efficace et Répartie | IUP MAI | 2003-04 | M1 | FI | Projets | 25 | 18h |
| Cryptographie et Sécurité | UFR imag | 2004-08 | M1 | FI | C/TD/TP | 25 | 18h |
| Compression | UFR imag | 2004-07 | M1 | FI | C/TD | 25 | 12h |
| Corps finis et applications | UFR imag | 2002-05 | M2 | FI | C | 12 | 18h |
| Théorie des codes | INP Télécom | 2001-08 | L3 | FI | C/TD | 80 | 18h |
| Mathématiques discrètes | Polytech' | 2003-04 | L3 | FI | C/TD | 80 | 18h |
| Maths110 | DLST UJF | 2002-04 | L1 | FI | TD | 40 | 54h |
| Processus Communicants | IUP MAI | 2002-03 | M1 | FI | C | 25 | 18h |
| Théorie des jeux à deux | Ensimag | 2000-02 | M1 | FI | Projets | 50 | 18h |
| Algorithmique | Ensimag | 2000-02 | M1 | FI | TD | 80 | 18h |
| Calcul Scientifique | Ensimag | 2000-02 | M1 | FI | C/TD | 80 | 32h |
| Méthodes Numériques | Polytech' | 1999-2004 | L3 | FI | C/TD | 80 | 32h |
| Algèbre | DSU UJF | 1997-2000 | L1 | FI | TD | 40 | 32h |
| Analyse | DSU UJF | 1997-2000 | L1 | FI | TD | 40 | 32h |

TABLE 1 – Volume horaire annuel par module enseigné depuis 1997

## Responsabilité de filière

Ces dernières années, je me suis largement investi dans le master 1 Mathématiques Appliquées et Industrielles. J'ai notamment pris en charge la réorganisation des enseignements de la partie informatique depuis 2003, et j'ai ensuite pris la responsabilité de cette filière de 2006 à 2009, puis de nouveau entre 2011 et 2015. Enfin, j'ai repris la responsabilité du Master 2 Cryptologie et Sécurité en septembre 2015.

## Développement du Master 2 Cryptologie et Sécurité

En effet, après ma thèse, je me suis formé à l'enseignement en codes correcteurs, compression et cryptologie et ai été impliqué dans la construction de la majorité des enseignements de ce domaine à Grenoble : en Master Informatique, en Master de Mathématiques Pures, en Master de Mathématiques

Appliquées et Industrielles, à l'école INP Telecom, à l'Ensimag, dans MOSIG –Master of Science in Informatics at Grenoble–, dans le Master Professionnel SCCI, Sécurité, cryptologie et codage de l'information (que j'ai contribué à monter avec Jean-Louis Roch et Franck Leprevost, dès 2001), puis dans la spécialité en apprentissage SAFE, Sécurité, Audit et Forensique pour l'Entreprise, en 2011. J'ai ensuite pris la responsabilité de cette filière, remaniée en Master 2 CyberSecurity, fin 2015.

## Enseignement et recherche en cryptologie et codes

Ces dernières années, mes compétences en calcul formel et en algorithmique de la théorie des nombres m'ont permis de me former à l'enseignement de la cryptologie, de la compression de données et de la correction d'erreur. La rédaction de supports de cours dans ces domaines s'est ensuite concrétisée par la publication, puis la traduction, d'un ouvrage à destination des Master [L66, L65] ainsi que par plusieurs chapitres d'un ouvrage de référence sur le sujet [L70, L71, L72].

## Développement à l'international

Enfin, avec Jean-Louis Roch, nous avons été amenés, à travers plusieurs contrats de formation [P88, P85, P84], à developper une filière internationale en Master 1 et 2 de Cryptologie et Sécurité à Grenoble. Cette formation a jeté les bases du Master 1 MOSIG et le Master 2 Cryptologie et Sécurité est devenu, par internationalisation des enseignements, le programme spécialisé SCIS (Security and Cryptology of Informatic Systems) du MOSIG, puis le Master 2 CyberSecurity de Grenoble. Nous allons actuellement vers un Master international Cybersecurity.

## Écoles et enseignements de $3^{\text{ième}}$ cycle

Cours Éliminations de Gauss modulaires et certificat d'inversibilité, Rencontres Arithmétique de l'Informatique Mathématique, Perpignan, février 2011.

Cours d'Algèbre linéaire Exacte, université d'Orsay, janvier 2006 et mars 2007.

Cours d'Algorithmique de la théorie des nombres à l'École d'été Cryptologie, Sécurité et Applications, Rabat, Maroc, 8-13 septembre 2003.

Cours d'Algèbre Linéaire creuse et LinBox à l'École d'été Outils de Calcul Symbolique Numérique Collaboratif, Giens, 17 septembre 2002.

Cours Calcul Formel, puis High-Performance Exact Computations. Master Recherche en Mathématiques Appliquées, université de Grenoble, 2002-2016.

Cours PKI, puis Architectures de Sécurité. Master Professionnel en Cryptologie et sécurité de l'information, université de Grenoble, depuis 2003.

Organisateur (avec Natacha Portier, Lyon) de l'École de Jeunes Chercheurs en Algorithmique et Calcul Formel (EJCACF'O4), du 29 mars au 2 avril 2004, à Grenoble.

# ACTIVITÉS DE RECHERCHE

## Calcul exact intensif

Ma recherche dans l'équipe CASYS du LJK porte principalement sur la conception, l'analyse et le développement d'algorithmes efficaces pour le calcul formel. Cette recherche se concrétise autour de plusieurs axes :

- Algèbre linéaire exacte [A1, A16, A2, T108, T107, A3, A4, A17, A5, A6, L69, A24, A8, A7, A27, A28, A53, A10, A12, A13, A31, A14, A50, A54, A57],
- Arithmétique, Sécurité, Cryptologie et Codes [A35, A36, A15, L68, A39, A38, L65, L64, A19, A44, A20, A46, A25, A26, A32, A9, A33, A29, A49, L66, L72, L71, L70],
- Systèmes symboliques-numériques [A21, A11, A55],
- Modèles de calcul et programmation orientée objet [A40, A41, B59, A22, A45, A23, B62, B60, A56, L73],
- Algorithmes parallèles [A18, A43, A30, A47, A48, A51, B63, A52, A58, B61],

ainsi que par plusieurs réalisations logicielles [S106, S99, S104, S100, S103, S102, S101, A37].

Ma recherche s'est également concrétisée au travers d'une quinzaine de projets de recherche dans ces thématiques :

**Algèbre linéaire exacte.**

1. 2012-2015 Projet ANR – **HPAC** [P82] : Calcul Algébrique Haute-Performance (coordinateur).
2. 2012-2014 équipe associée INRIA-NSF – **QOLAPS** [P78] : Quantfier elimination, Optimization, Linear Algebra and Polynomial Systems.
3. Depuis 1998 Projet international CNRS-NSF-NSERC **LINBOX** [S100] : algèbre linéaire creuse.

**Conception et modélisation logicielles, algorithmique parallèle.**

1. 2015-2019 Projet Européen – **OPENDREAMKIT** [P80] : Open Digital Research Environment Toolkit for the Advancement of Mathematics.
2. 2010-2012 Projet CNRS-PEPS – //**INBOX** [P89] : Outils logiciels pour le calcul algébrique haute performance.
3. 2005-2008 Projet Région dans le Cluster ISLE [P91] : **CALCUL HAUTES PERFORMANCES ET INFORMATIQUE DISTRIBUÉE**.
4. 2005-2007 Projet IMAG – **AHA** [P96] : Algorithmes Hybrides Adaptatifs (co-responsable).
5. 2003-2004 Projet IMAG – **INCA** [P97] : Interfaces pour le calcul formel (co-responsable).

**Sécurité, cryptologie, codes, arithmétique.**

1. 2014-2018 Projet Investissement d'Avenir – **ARAMIS** [P86] : Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles.
2. 2011-2012 Projet Grenoble universités – **MPLLC** [P93] : Multi-Precision Library for Lattices and Cryptography (co-responsable).
3. 2009-2011 Projet Ministère de l'industrie – **SHIVA** [P87] : Secured Hardware Immune Versatile Architecture.
4. 2008-2009 Projet Grenoble universités – **PALOALTO** [P95] : Plateforme d'Attaques LOgicielles par ALgorithmes et Techniques Optimisés pour architectures Multi-Coeurs Parallèles (co-responsable).

5. 2006-2009 Projet ANR – **BGPR-SAFESCALE** [P83] : certification et tolérance aux fautes sur grille de calcul.

**Algorithmes symboliques-numériques.**

1. 2008-2009 Projet Grenoble universités – **CARESSE** [P94] : Contrôle et Analyse de Réseaux de Systèmes Dynamiques Évolutifs.
2. 2005-2008 Projet Région – **CALCUL CELLULAIRE** [P92].
3. 2002-2006 Laboratoire Franco-Chinois [P79].
4. 2003-2004 Projet européen – **COMPUTATION AND CONTROL** [P81].
5. 2002-2003 Projet CNRS – **ANALYSE DES SYSTÈMES HYBRIDES** [P90] (coordinateur).

# RAYONNEMENT

## Activité éditoriales et de conseil scientifique

**Éditeur associé** du journal *ACM Communications in Computer Algebra*, depuis 2006.

**Conseil scientifique national et international**

- FWF - *Fonds zur Förderung der wissenschaftlichen Forschung* (Austrian Science Fund), 2016, 2012.
- Inria, 2016.
- ANR - Agence nationale de la recherche, 2017, 2016, 2015.
- INFORMS - *Institute for Operations Research and the Management Sciences*, USA, 2014.
- NSA-AMS - *joint American Mathematical Society / National Security Agency, Mathematical Sciences Program*, USA, 2013.
- SCCyPhy - équipe-action Security and Cryptology for CyberPhysical system, (membre du comité scientifique), France, depuis 2013.
- NSERC - *Natural Sciences and Engineering Research Council of Canada*, 2016, 2013.
- AERES - Agence d'évaluation de la recherche et de l'enseignement supérieur, (évaluation des laboratoires LAGIS, LIFL et de leur fusion, le CRISTAL), 2013.
- *Grantová agentura České republiky* (Agence Tchèque de subventions), 2011.
- JNCF - Journées nationales de Calcul Formel, membre du comité scientifique depuis 2010.
- SIGSAM - *ACM Special Interest Group on Symbolic and Algebraic Manipulation*, USA, advisory board member at large (membre élu pour trois ans, 2007-2010).

**Sociétés savantes**

- Vice-président élu de l'association internationale ACM SIGSAM, depuis 2013.
- International Linear Algebra Society (ILAS) depuis 2013.
- Association for Computing Machinery (ACM) depuis 2000.

## Comités de programmes et comités de lecture internationaux

— Comités de programmes : *PASCO 2017, 2015 (chair), 2010, 2007* ; *ISSAC 2016, 2013, 2010, 2009* ; *GreHack 2017, 2016* ; *LCASNC 2015 (chair)* ; *ICMC 2013* ; *PARCA 2010* ; *TC 2006* ; *OSAGC 2005*.

— Comités de lecture : *Journal of Symbolic Computation* (2016, 2015, 2013, 2008, 2006, 2003, 2002, 2000) ; *ACM Transactions on Mathematical Software* (2016,2010,2009) ; *IEEE Trans. on Computers* (2017) ; *Proyecciones journal of mathematics* (2017) ; *Mathematical Reviews* (2017,2016) ; *Discrete Applied Mathematics* (2012, 2010) ; *Engineering Science and Technology, an International Journal* (2016) ; *Special Matrices* (2014) ; *Annals of telecommunications* (2013) ; *Mathematics and Computers in Simulation* (2012) ; *Parallel Computing* (2011) ; *The Computer Journal* (2013, 2011) ; *Mathematical Structures in Computer Science* (2010) ; *Applicable Algebra in Engineering, Communication and Computing* (2010) ; *ACM Communications in Computer Algebra* (2013, 2011, 2010, 2008, 2007, 2006) ; *Missouri Journal of Mathematical Sciences* (2009) ; *Information Sciences* (2008) ; *Journal of Complexity* (2004) ; *Theoretical Computer Science Algorithms* (2003) ; *Journal of Computational and Applied Mathematics* (2002).

— Rapporteur pour les conférences internationales : *ISSAC 2016, 2013, 2012, 2010, 2009, 2008, 2007, 2005, 2004, 2003, 2002* ; *LCASNC 2015* ; *CASC 2013, 2003* ; *ASCM 2012* ; *ICMS 2010* ; *PASCO 2017, 2015, 2010, 2007* ; *PARCA 2010* ; *IEEE ARITH 2007* ; *SNC 2007* ; *SYNACS 2006* ; *WWCA 2006* ; *Transgressive Computing 2006* ; *CALCULEMUS 2006* ; *IEEE HPCS 2005* ; *STACS 2002* ; *IPDPS 2001*.

## Direction adjointe du Laboratoire Jean Kuntzmann

Du 1er janvier 2014 au 31 décembre 2016, j'ai été directeur adjoint du Laboratoire Jean Kuntzmann (UMR 5223), en charge du département Modèles et Algorithmes Déterministes. Le département regroupe 6 équipes de recherche et 130 personnes s'intéressant aux équations aux dérivées partielles, au calcul formel, à l'optimisation, aux systèmes dynamiques, aux nano-systèmes ou encore aux mathématiques de la décision.
Membre de l'équipe de direction du laboratoire, j'ai donc été notamment en charge du budget du département MAD, de son animation scientifique, de son rapport d'évaluation pour l'HCERES, ou encore de relations entre le LJK et le pôle de recherche MSTIC de l'université, etc.

## Responsabilité d'équipe de recherche

Durant le quadriennal 2006-2009, et depuis 2017, je suis responsable de l'équipe CASYS (Calculs Algébriques et Systèmes Dynamiques) au sein du département Modèles et Algorithmes Déterministes du LJK. L'équipe regroupe 12 chercheurs permanents et une dizaine de doctorants, post-doctorants ou ingénieurs, s'intéressant au calcul exact (calcul formel, arithmétique, cryptologie), à l'analyse et au contrôle de systèmes dynamiques hybrides (symboliques/exacts/numériques) ainsi qu'à la modélisation informatique du calcul.

## Commission de spécialistes et conseil d'UFR

- Titulaire élu de la commission de spécialistes de la section 26, mathématiques appliquées, de l'université Joseph Fourier, 2003-2008.
- Titulaire élu du conseil d'UFR informatique et mathématiques appliquées, de l'université Joseph Fourier, 2007-2011.

## Responsabilité des moyens informatiques

De 2002 à 2007, puis depuis 2011, je suis responsable des moyens informatiques de l'équipe MOSAIC, puis CASYS du LJK. En son sein, je gère un parc d'une vingtaine de stations PC (des Linux Debian/Mandrake/Ubuntu, des Windows XP/Vista/Win7, des Apple powerbook), DEC alpha et serveurs SUN solaris.

## Prix, distinctions

- *Best Paper Award*, SECRYPT 2016.
- ACM SIGSAM *Distinguished Paper Award*, ISSAC 2015.
- Titulaire de la PEDR 2005-2009, de la PES 2009-2013, de la PEDR 2014-2018.
- Accessit au concours général de mathématiques 1992.

## Organisation de conférences

LCASNC 2015, ILAS2013, ACM ISSAC2012, SIAM AAG2011, ACM ISSAC2011, ACM PASCO2010, DubLinBox2010, JNCF2010, ACM ISSAC2009, JNCF2008, ACM ISSAC2006, Transgressive Computing 2006, SIAM PPSC2006, CalSym2005, EJCACF2004, JNCF2003.

## Communications, invitations et séjours de recherche internationaux

**36.** 15 – 25 juillet 2016 : Milestones in Computer Algebra (MICA 2016), Waterloo, Canada.

**35.** Octobre-Novembre 2015 : Invitation au Fields Institute, Toronto, dans le cadre du semestre thématique sur le calcul formel.

**34.** 26 – 31 Octobre 2015 : Essentially Optimal Certificates in Linear Algebra. Workshop on Linear Computer Algebra and Symbolic-Numeric Computation, Fields Institute, Toronto, Canada.

**33.** 23 – 25 juillet 2014 : Matrix multiplication over word-size prime fields using Bini's approximate formula (avec Brice Boyer). The 39th International Symposium on Symbolic and Algebraic Computation (ISSAC'14), Kobe, Japon.

**32.** 2 – 4 juillet 2014 : Parallel computation of echelon forms (avec Clément Pernet et Ziad Sultan). 8th International Workshop on Parallel Matrix Algorithms and Applications (PMAA'14), Lugano, Suisse.

**31.** 18 – 21 février 2014 : Parallel computation of rank profiles (avec Clément Pernet et Ziad Sultan). 16th SIAM Conference on Parallel Processing for Scientific Computing (SIAM'PP14), Portland, USA.

**30.** 13 – 20 décembre 2013 : Collaboration avec Erich Kaltofen à Raleigh, North Carolina, USA.

**29.** 1 – 7 juin 2013 : Reducing memory consumption in Strassen-like matrix multiplication (avec Brice Boyer). 18th Conference of the International Linear Algebra Society (ILAS 2013), Providence, USA.

**28.** 17 mars 2013 : Verifiability in e-Auction Protocols (avec Jannik Dreier, Hugo Jonker et Pascal Lafourcade). 1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013), Rome, Italie.

**27.** 5 – 14 octobre 2011 : Collaboration avec Erich Kaltofen et session *Exact linear algebra and algebraic topology* à "SIAM Conference on Applied Algebraic Geometry", Raleigh, North Carolina, USA.

**26.** 13 – 17 Septembre 2010 : *LinBox founding scope allocation, parallel building blocks, and template separate compilation* (avec Thiérry Gautier, Clément Pernet et B. David Saunders). International Congress on Mathematical Software, Kobe, Japon.

**25.** 28 – 29 Août 2010. States and exceptions are dual effects (avec Dominique Duval, Laurent Fousse et Jean-Claude Reynaud). International Workshop on Categorical Logic . Masaryk University, Brno, république Tchèque.

**24.** Août 2009 – Juillet 2010 : Professeur invité au Claude Shannon Institute, University College Dublin, Irlande.

**23.** 31 mai – 4 juin 2010 : *CRA computations on multicore architectures* (avec Thierry Gautier). DubLinBox. Dublin, Irlande.

**22.** 16 – 18 Mai 2010 : *Finite semifields and the Frobenius normal form*. The Claude Shannon Institute Workshop on Coding and Cryptography. Cork, Irlande.

**21.** 18 Janvier 2010 : *Primitive roots, spiral permutations and lyric poetry of troubadours*. UCD School of Mathematical Sciences, Algebra seminars. Dublin, Irlande.

**20.** 22 Octobre 2009 : *Introspective algorithms for very fast exact linear algebra*. Complex and Adaptive Systems Laboratory. Dublin, Irlande.

**19.** 2 – 4 Septembre 2009 : *Exact linear algebra for cryptology and codes*. WCS'09 : Workshop on Coding and Systems. Dublin, Irlande.

**18.** 28 – 31 Août 2009 : *Betti number and torsions via exact linear algebra*. Invitation du gouvernement Américain au Sandia National Laboratories, CAT'09 : CSRI Workshop on Combinatorial Algebraic Topology. Santa FE, NM, USA.

**17.** 25-28 Juin 2009. Linear Algebra Modulo Tiny Primes (avec B. David Saunders et Brian Youse). ACA'09 : 2009 IMACS Conference on Applications of Computer Algebra: High Performance Computer Algebra. Montreal, Canada.

**16.** 22 mars 2009. Sequential products for effects (avec Dominique Duval et Jean-Claure Reynaud). ACCAT'09 : Applied and Computational Category Theory. York, UK.

**15.** 10 – 15 Octobre 2008 : *Simultaneous Modular Reduction and Kronecker Substitution for Small Finite Fields*, SAGE Days 10, Nancy, France.

**14.** 1 – 3 Septembre 2006 : *Exact Linear Algebra Software*, International Congress on Mathematical Software, Castro Urdiales, Espagne.

**13.** 2 – 7 Juillet 2006 : *Adaptive and Hybrid Algorithms*, Dagstuhl-Seminar 06271/1, Allemagne.

**12.** 1 – 6 Octobre 2005 : LINBOX*-1.0.0, fast algorithms made efficient*, Challenges in Linear and Polynomial Algebra in Symbolic Computation Software, Banff, Canada.

**11.** 24 – 27 Juillet 2005 : LINBOX*-1.0.0, a demonstration*, ISSAC 2005 Software Exhibitions, Beijing, Chine.

**10.** 8 – 13 Septembre 2003 : *Algorithmique de la Théorie des nombres*. Cryptologie, Sécurité et Applications ; collaboration avec Saïd El Hajji, de l'université Mohammed V Agdal, Rabat, Maroc.

**9.** 1 – 9 Août 2003 : collaboration avec Zhendong Wan, de l'université Drexel, Pennsylvannie, USA.

8. Décembre 2002 et août 2001 : collaboration avec Mark Giesbrecht à l'University of Western Ontario, London, Canada.
7. 1 – 10 juillet 2002 : collaboration avec Lijun Yang, de l'université de Tsinghua à Beijing, Chine.
6. 25 – 28 Juin 2002 : *Exact sparse linear algebra*, ACA'2002, Volos, Grèce.
5. Mai 2002 : collaboration avec Volkmar Welker, de l'université Technique de Marburg, Allemagne.
4. Août 2001 : *FFLAS, finite field linear algebra subroutines*, université de Waterloo, Ontario, Canada.
3. Octobre 1999 : collaboration avec Günter M. Ziegler et Volkmar Welker, TU Berlin, Allemagne.
2. Avril 1999 : collaboration avec Erich Kaltofen, North Carolina State University, Raleigh, USA.
1. Entre juillet 1998 et août 2000 : Travail avec B. David Saunders sur le calcul efficace de formes normales de Smith de matrices entières (8 mois à l'U. of Delaware, USA).

## Communications, invitations et séminaires nationaux

49. *Architectures de sécurité*. Formation @GP, Grenoble, France, 14-15 juin 2016.
48. *Architectures PKI et communications sécurisées* (avec Pascal Lafourcade et Patrick Redon). RESSI 2016, Toulouse, France, 10-13 mai 2016.
47. *Comment vérifier les résultats de calculs externalisés ?*. Séminaire sur la Confiance Numérique, Clermont-Ferrand, France, 3 Décembre 2015.
46. *Sécuriser ses communications avec une architecture PKI* (avec Pascal Lafourcade et Patrick Redon). OZSSI 2015, Clermont-Ferrand, France, 6 octobre 2015.
45. *Attaques par perturbation sur RSA embarqué*. Formation Tiempo-Secure, Montbonnot, France, 15-17 juin 2015.
44. *Generating S-Boxes from semi-fields pseudo-extensions*. SDTA 2014, Clermont-Ferrand, France, 4-5 Décembre 2014.
43. *Noyaux efficaces d'algèbre linéaire exacte*. JNCF 2014, Luminy, France, novembre 2014.
42. *Approches creuses pour l'analyse exacte de motifs dans des séquences générées par une source Markovienne*. Séminaire SPOC, IMB, Dijon, 21 mai 2014.
41. *Interactive certificates in linear algebra*. LIP6, Paris, 19 mai 2014.
40. *Vérifier l'algèbre linéaire en temps linéaire*. Séminaire Bipop-Casys, LJK, Grenoble, 15 mai 2014.
39. *Approches creuses pour l'analyse exacte de motifs dans des séquences générées par une source Markovienne*. Séminaire AriC, LIP, Lyon, 13 juin 2013.
38. *Towards parallel linear algebra kernels over finite fields*. JNCF 2013, Luminy, France, 13 mai 2013.
37. *Computer Algebra Patterns : vers une architecture efficace, générique et pérenne de logiciels mathématiques*. Séminaire Bipop-Casys, LJK, 20 janvier 2012.
36. *Sur la complexité du calcul du polynôme caractéristique*, Séminaire SALSA, LIP6, Paris, 12 avril 2011.
35. *Approches creuses pour la distribution de motifs dans l'ADN et le protéome*. Séminaire ARITH, LIRMM, Montpellier, 30 mars 2011.
34. *Éliminations de Gauß modulaires et certificat d'inversibilité*. Cours au RAIM 2011. Perpignan, 7-10 février 2011.
33. *Codes correcteurs et espaces de matrices à rang constant*. LJK, Séminaire secpol, 2 décembre 2010.
32. *Sequential computation and cartesian effect categories*. Categorical Computer Science. Grenoble, 26 novembre 2009.
31. *Polynôme caractéristique de matrices creuses*, LJK Séminaire MAD, Grenoble, 25 juin 2009.
30. *Attaque par perturbation sur RSA embarqué*, LJK Séminaire MAD, 18 décembre 2008.
29. *Arithmétique compressée pour des petits corps finis*, RAIM 2008, Lille, 3 juin 2008.
28. *Comment casser RSA et le logarithme discret ?*, LJK Séminaire MAD, Grenoble, 31 janvier 2008.
27. *Compromis temps/mémoire en algèbre linéaire dense sur des corps finis*, GDR Informatique Mathématique, Paris Diderot, 24 janvier 2008.
26. *Outils pour un intergiciel générique*, Journées Nationales de Calcul Formel 2007, Marseille, 1 février 2007.
25. *Résolution exacte de problèmes mal conditionnés*, Institut Camille Jordan, Lyon, 30 mars 2006.
24. *Racines primitives industrielles*, séminaire de cryptologie, Institut Fourier, Grenoble, 9 février 2006.
23. *Dessiner les calculs, modélisation diagrammatique de la bibliothèque* LinBox, Calculs Symboliques, Grenoble, 16 décembre 2005.
22. *Le bon résultat tout de suite*. Algèbre linéaire exacte, Ensimag, Grenoble, 14 décembre 2005.

**21.** *DML, a diagrammatic modeling language for object programming*, Journées Nationales de Calcul Formel, Luminy, 24 novembre 2005.

**20.** LinBox*-1.0.0 : exact algorithms beat numerical routines for ill-conditioned problems*, LMC, séminaire Mosaic, Grenoble, 17 novembre 2005.

**19.** LinBox*-1.0.0 : a tutorial*, Open Software for Algebraic and Geometric computation, université de Nice Sophia Antipolis, 5 septembre 2005.

**18.** *Adaptive FFLAS*, laboratoire ID, Montbonnot, 30 mai 2005.

**17.** *Évaluation dynamique en algèbre linéaire entière*, LIP6, Paris, 17 décembre 2003.

**16.** *Topologie cellulaire et forme normale de Smith*, École Normale Supérieure de Lyon, 18 novembre 2003.

**15.** *Codes correcteurs d'erreurs*, Conférences Midisciences, Grenoble, 25 mars 2003.

**14.** *Tutoriel* LinBox, École d'été, Outils de Calcul Symbolique Numérique Collaboratif, Giens, 17 septembre 2002.

**13.** *Calcul de groupes d'homologie de complexes simpliciaux : forme normale de Smith entière*, université de Montpellier II, 5 juin 2002.

**12.** LinBox*, certification et sécurisation sur grille*, laboratoire Informatique et Distribution, Grenoble, 16 mai 2002.

**11.** LinBox*, une bibliothèque générique efficace pour le calcul formel*, Projet INRIA GALAAD, Sophia Antipolis, 29 avril 2002.

**10.** *Calcul d'Homologie de Complexes simpliciaux par l'algèbre linéaire*, Institut Fourier, Grenoble, 4 avril 2002.

**9.** *Indigo, une bibliothèque générique pour les systèmes hybrides*, Groupe de travail Systèmes Hybrides, MOSAIC, 7 février 2002.

**8.** *Analysis and Simulation of ODE using Hybrid Systems*, (avec Antoine Girard), European IST project CC (Control and Computation), Kick-Off meeting, Grenoble, 24-25 janvier 2002.

**7.** *Triangulation de Delaunay pour les systèmes hybrides*, Atelier SQUASH, Verimag, 4 décembre 2001.

**6.** *Arithmétique efficace sur les corps finis, ou comment calculer exactement aussi vite qu'en numérique*, LMC, équipe MOSAIC, Grenoble, 25 octobre 2001.

**5.** *Calcul du rang et de la forme normale de Smith de très grandes matrices creuses entières*, université de Lyon, Gerland, 21 octobre 2001.

**4.** *Forme normale de Smith : expérience avec de grandes matrices creuses*, Projet INRIA GALAAD, Sophia Antipolis, 30 mai 2001.

**3.** *Valence : a blackbox method for the integer Smith normal form*, LMC, séminaire de calcul formel, 22 juin 2000.

**2.** *Athapascan-1, interface de programmation pour la répartition dynamique de charge*, Université des sciences et technologies de Lille, 26 novembre 1999.

**1.** *A new integer Smith form algorithm*, LMC, séminaire de Parallélisme, Grenoble, 14 décembre 1998.

# PUBLICATIONS

http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/publications.html

## Conférence ISSAC (**ACM International Symposium on Symbolic and Algebraic Computation**)

[A1] Jean-Guillaume Dumas, Erich Kaltofen, Gilles Villard et Lihong Zhi. – Polynomial time interactive proofs for linear algebra with exponential matrix dimensions and scalars given by polynomial time circuits. Dans : **ISSAC'2017** [120 - Safey El Din (2017)], pages 125–132.

[A2] Jean-Guillaume Dumas, David Lucas et Clément Pernet. – Certificates for triangular equivalence and rank profiles. Dans : **ISSAC'2017** [120 - Safey El Din (2017)], pages 133–140.

[A3] Jean-Guillaume Dumas, Erich Kaltofen, Emmanuel Thomé et Gilles Villard. – Linear time interactive certificates for the minimal polynomial and the determinant of a sparse matrix. Dans : **ISSAC'2016** [111 - Gao (2016)], pages 199–206.

[A4] Jean-Guillaume Dumas, Clément Pernet et Ziad Sultan. – Computing the rank profile matrix. Dans : **ISSAC'2015** [122 - Yokoyama (2015)], pages 149–156. **Distinguished paper award**.

[A5] Jean-Guillaume Dumas et Erich Kaltofen. – Essentially optimal interactive certificates in linear algebra. Dans : **ISSAC'2014** [119 - Nabeshima (2014)], pages 146–153.

[A6] Jean-Guillaume Dumas, Clément Pernet et Ziad Sultan. – Simultaneous computation of the row and column rank profiles. Dans : **ISSAC'2013** [115 - Kauers (2013)], pages 181–188.

[A7] Brice Boyer, Jean-Guillaume Dumas, Clément Pernet et Wei Zhou. – Memory efficient scheduling of Strassen-Winograd's matrix multiplication algorithm. Dans : **ISSAC'2009** [116 - May (2009)], pages 135–143.

[A8] Jean-Guillaume Dumas, Clément Pernet et B. David Saunders. – On finding multiplicities of characteristic polynomial factors of black-box matrices. Dans : **ISSAC'2009** [116 - May (2009)], pages 55–62.

[A9] Jean-Guillaume Dumas. – Q-adic transform revisited. Dans : **ISSAC'2008** [113 - Jeffrey (2008)], pages 63–69.

[A10] Jean-Guillaume Dumas, Clément Pernet et Zhendong Wan. – Efficient computation of the characteristic polynomial. Dans : **ISSAC'2005** [114 - Kauers (2005)], pages 140–147.

[A11] Jean-Guillaume Dumas et Aude Rondepierre. – Algorithms for symbolic/numeric control of affine dynamical systems. Dans : **ISSAC'2005** [114 - Kauers (2005)], pages 277–284.

[A12] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – FFPACK: Finite field linear algebra package. Dans : **ISSAC'2004** [112 - Gutierrez (2004)], pages 119–126.

[A13] Jean-Guillaume Dumas, Thierry Gautier et Clément Pernet. – Finite field linear algebra subroutines. Dans : **ISSAC'2002** [117 - Mora (2002)], pages 63–74.

[A14] Jean-Guillaume Dumas, B. David Saunders et Gilles Villard. – Integer Smith form via the Valence: experience with large sparse matrices from Homology. Dans : **ISSAC'2000** [121 - Traverso (2000)], pages 95–105.

## Revues internationales avec comité de lecture

[A15] Jean-Guillaume Dumas, Pascal Lafourcade, Jean-Baptiste Orfila et Maxime Puys. – Dual protocols for private multi-party matrix multiplication and trust computations. **Computers & Security**, n°71, novembre 2017, pages 51–70.

[A16] Jean-Guillaume Dumas, Clément Pernet et Ziad Sultan. – Fast computation of the rank profile matrix and the generalized Bruhat decomposition. **Journal of Symbolic Computation**, volume 83, novembre–décembre 2017, pages 187–210.

[A17] Brice Boyer et Jean-Guillaume Dumas. – Matrix multiplication over word-size modular rings using approximate formulae. **ACM Transactions on Mathematical Software**, volume 42, n° 3, juin 2016, pages 20 :1–20 :12.

[A18] Jean-Guillaume Dumas, Thierry Gautier, Clément Pernet, Jean-Louis Roch et Ziad Sultan. – Recursion based parallelization of exact dense linear algebra routines for Gaussian elimination. **Parallel Computing**, volume 57, septembre 2016, pages 235–249.

[A19] Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. – Brandt's fully private auction protocol revisited. **Journal of Computer Security**, volume 23, n° 5, 2015, pages 587–610.

[A20] Jean-Guillaume Dumas. – On Newton-Raphson iteration for multiplicative inverses modulo prime powers. **IEEE Transactions on Computers**, volume 63, n° 8, août 2014, pages 2106–2109.

[A21] Jean-Guillaume Dumas et Grégory Nuel. – Sparse approaches for the exact distribution of patterns in long state sequences generated by a Markov source. **Theoretical Computer Science**, volume 479, avril 2013, pages 22–42.

[A22] Jean-Guillaume Dumas, Dominique Duval, Laurent Fousse et Jean-Claude Reynaud. – A duality between exceptions and states. **Mathematical Structures in Computer Science**, volume 22, n° 4, août 2012, pages 719–722.

[A23] Jean-Guillaume Dumas, Dominique Duval et Jean-Claude Reynaud. – Cartesian effect categories are Freyd-categories. **Journal of Symbolic Computation**, volume 46, n° 3, mars 2011, pages 272–293.

[A24] Jean-Guillaume Dumas, Laurent Fousse et Bruno Salvy. – Simultaneous modular reduction and Kronecker substitution for small finite fields. **Journal of Symbolic Computation**, volume 46, n° 7, juillet 2011, pages 823–840.

[A25] Jean-Guillaume Dumas, Rod Gow et John Sheekey. – Rank properties of subspaces of symmetric and hermitian matrices over finite fields. **Finite Fields and their Applications**, volume 17, n° 6, novembre 2011, pages 504–520.

[A26] Jean-Guillaume Dumas, Rod Gow, Gary McGuire et John Sheekey. – Subspaces of matrices with special rank properties. **Linear Algebra and its Applications**, volume 433, n° 1, juillet 2010, pages 191–202.

[A27] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – Dense linear algebra over prime fields. **ACM Transactions on Mathematical Software**, volume 35, n° 3, novembre 2008, pages 1–42.

[A28] Jean-Guillaume Dumas. – Bounds on the coefficients of the characteristic and minimal polynomials. **Journal of Inequalities in Pure and Applied Mathematics**, volume 8, n° 2, avril 2007. – 6 pp, art. 31.

[A29] Jacques Dubrois et Jean-Guillaume Dumas. – Efficient polynomial time algorithms computing industrial-strength primitive roots. **Information Processing letters**, volume 97, n° 2, janvier 2006, pages 41–45.

[A30] Jean-Guillaume Dumas et Jean-Louis Roch. – On parallel block algorithms for exact triangularizations. **Parallel Computing**, volume 28, n° 11, novembre 2002, pages 1531–1548.

[A31] Jean-Guillaume Dumas, B. David Saunders et Gilles Villard. – On efficient sparse integer matrix Smith normal form computations. **Journal of Symbolic Computation**, volume 32, n° 1/2, juillet–août 2001, pages 71–99.

---

Revues nationales avec comité de lecture

---

[A32] Jean-Guillaume Dumas. – Les rayons des permutations spirales. **Mathématiques et Sciences Humaines**, volume 192, n° 4, 2010, pages 5 – 27.

[A33] Jean-Guillaume Dumas. – Caractérisation des quenines et leur représentation spirale. **Mathématiques et Sciences Humaines**, volume 184, n° 4, 2008, pages 9 – 23.

[A34] Benoît Badrignans, Vincent Danjean, Jean-Guillaume Dumas, Philippe Elbaz-Vincent, Sabine Machenaud, Jean-Baptiste Orfila, Florian Pebay-Peyroula, François Pebay-Peyroula, Marie-Laure Potet, Maxime Puys, Jean-Luc Richier et Jean-Louis Roch. – Security architecture for point-to-point splitting protocols. Dans : **IEEE World Congress on Industrial Control Systems Security, Cambridge, UK**, 11–14 décembre 2017, page 8.

[A35] Jean-Guillaume Dumas, Pascal Lafourcade, Francis Melemedjian, Jean-Baptiste Orfila et Pascal Thoniel. – LocalPKI: A user-centric formally proven alternative to PKIX. Dans : **Proceedings of the 14th International Conference on Security and Cryptography (SECRYPT 2017), Madrid, Spain**, Pierangela Samarati éd., 24–26 juillet 2017. – *ICETE 2017*, pages 187–199. – SciTePress.

[A36] Jean-Guillaume Dumas et Vincent Zucca. – Prover efficient public verification of dense or sparse/structured matrix-vector multiplication. Dans : **ACISP 2017, 22nd Australasian Conference on Information Security and Privacy**, Josef Pieprzyk et Suriadi Suriadi éd., 3–7 juillet 2017. – *LNCS*, volume 10343, pages 115–134. – Springer.

[A37] Christophe Chabot Alexis Breust, Jean-Guillaume Dumas, Laurent Fousse et Pascal Giorgi. – Recursive double-size fixed precision arithmetic. Dans : **5th International Congress on Mathematical Software (ICMS 2016)**, G.-M. Greuel, T. Koch, P. Paule et A. Sommese éd., 11–15 juillet 2016. – *LNCS*, volume 9725, pages 223–231. – Springer.

[A38] Xavier Bultel, Jannik Dreier et Jean-Guillaume Dumas Pascal Lafourcade. – Physical zero-knowledge proofs for Akari, Kakuro, KenKen and Takuzu. Dans : **8th International conference on Fun with algorithms (FUN 2016)**, Erik D. Demaine et Fabrizio Grandoni éd., 8–10 juin 2016. – *Leibniz International Proceedings in Informatics (LIPIcs)*, volume 49, pages 8 :1–8 :20. – Dagstuhl, Germany.

[A39] Jean-Guillaume Dumas, Pascal Lafourcade, Jean-Baptiste Orfila et Maxime Puys. – Private multi-party matrix multiplication and trust computations. Dans : **Proceedings of the 13th International Conference on Security and Cryptography (SECRYPT 2016), Lisbon, Portugal, July 26-28, 2016**, Pierangela Samarati éd., 26–28 juillet 2016. – *ICETE 2016*, volume 4, pages 61–72. – SciTePress. **Best paper award**.

[A40] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici, Damien Pous et Jean-Claude Reynaud. – Relative Hilbert-Post completeness for exceptions. Dans : **MACIS 2015, Sixth International Conference on Mathematical Aspects of Computer and Information Sciences**, S. Ilias Kotsireas, M. Siegfried Rump et K. Chee Yap éd., 11–13 novembre 2015. – *LNCS*, pages 596–610. – Springer.

[A41] Brice Boyer, Jean-Guillaume Dumas, Pascal Giorgi, Clément Pernet et B. David Saunders. – Elements of design for containers and solutions in the LinBox library. Dans : **ICMS'2014, Proceedings of the 2014 International Congress of Mathematical Software, Seoul, Korea**, Hoon Hong et Chee K. Yap éd., 5–9 août 2014. – *LNCS*, volume 8592, pages 654–662. – Springer.

[A42] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici et Jean-Claude Reynaud. – Certified proofs in programs involving exceptions. Dans : **CICM-WIP'2014, Proceedings of the 2014 Conference on Intelligent Computer Mathematics Work in Progress, Coimbra, Portugal**, Matthew England, James Davenport, Paul Libbrecht, Andrea Kohlhase, Michael Kohlhase, Walther Neuper, Pedro Quaresma, Josef Urban, Alan Sexton, Petr Sojka et Stephen Watt éd., 7–11 juillet 2014. – *CEUR Workshop Proceedings*, pages 1–16. – Aachen.

[A43] Jean-Guillaume Dumas, Thierry Gautier, Clément Pernet et Ziad Sultan. – Parallel computation of echelon forms. Dans : **Euro-Par'2014, Proceedings of the 20th international conference on parallel processing, Porto, Portugal**, Fernando Silva, Inês Dutra et Vítor Santos Costa éd., 25–29 août 2014. – *LNCS*, volume 8632, pages 499–510. – Springer.

[A44] Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. – Attacking privacy in a fully private auction protocol. Dans : **AfricaCrypt'2013, Proceedings of the sixth International**

**Conference on Cryptology in Africa, Cairo, Egypt**, Amr Youssef et Abderrahmane Nitaj éd., 22–24 juin 2013. – *LNCS*, volume 7918, pages 88–106. – Springer.

[A45] Jean-Guillaume Dumas, Dominique Duval, Laurent Fousse et Jean-Claude Reynaud. – Decorated proofs for computational effects: States. Dans : **ACCAT'2012, Proceedings of the Seventh Workshop on Applied and Computational Category Theory (co-ETAPS 2012), Tallinn, Estonia**, Ulrike Golas et Thomas Soboll éd., 1 avril 2012. – *Electronic Proceedings in Theoretical Computer Science*, volume 93, pages 45–59.

[A46] Jean-Guillaume Dumas et Hicham Hossayni. – Matrix powers algorithm for trust evaluation in PKI architectures. Dans : **STM'2012, Proceedings of the eigth International Workshop on Security and Trust Management (co-ESORICS 2012), Pisa, Italy**, Audun Jøsang, Pierangela Samarati et Marinella Petrocchi éd., 13–14 septembre 2012. – *LNCS*, volume 7783, pages 129–144. – Springer.

[A47] Brice Boyer, Jean-Guillaume Dumas et Pascal Giorgi. – Exact sparse matrix-vector multiplication on GPU's and multicore architectures. Dans : **PASCO'10** [118 - Moreno-Maza et Roch (2010)], pages 80–88.

[A48] Jean-Guillaume Dumas, Thierry Gautier et Jean-Louis Roch. – Generic design of chinese remaindering schemes. Dans : **PASCO'10** [118 - Moreno-Maza et Roch (2010)], pages 26–34.

[A49] Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas et Louis Goubin. – Fault attacks on RSA public keys: Left-to-right implementations are also vulnerable. Dans : **CTRSA'2009, Proceedings of the RSA Conference 2009, Cryptographers' Track, San Francisco, USA**, Marc Fischlin éd., 20–24 avril 2009. – *LNCS*, volume 5473, pages 414–428. – Springer.

[A50] Jean-Guillaume Dumas, Laurent Fousse et Bruno Salvy. – Compressed modular matrix multiplication. Dans : **Milestones in Computer Algebra 2008, Tobago**, Mark Giesbrecht et Stephen Watt éd., 1–3 mai 2008, pages 133–140.

[A51] Jean-Guillaume Dumas, Pascal Giorgi, Philippe Elbaz-Vincent et Anna Urbańska. – Parallel computation of the rank of large sparse matrices from algebraic k-theory. Dans : **PASCO'07, Proceedings of the 3rd ACM International Workshop on Parallel Symbolic Computation**, Marc Moreno-Maza et Stephen Watt éd., 26–27 juillet 2007. Pages 43–52. – Waterloo University, Ontario, Canada.

[A52] Van-Dat Cung, Vincent Danjean, Jean-Guillaume Dumas, Thierry Gautier, Guillaume Huard, Bruno Raffin, Christophe Rapine, Jean-Louis Roch et Denis Trystram. – Adaptive and hybrid algorithms: classification and illustration on triangular system solving. Dans : **TC'2006** [L77], pages 131–148.

[A53] Jean-Guillaume Dumas et Anna Urbańska. – An introspective algorithm for the determinant. Dans : **TC'2006** [L77], pages 185–202.

[A54] Jean-Guillaume Dumas. – Efficient dot product over finite fields. Dans : **CASC'2004, Proceedings of the seventh International Workshop on Computer Algebra in Scientific Computing, Saint Petersburg, Russia**, Victor G. Ganzha, Ernst W. Mayr et Evgenii V. Vorozhtsov éd., 12–19 juillet 2004. Pages 139–154. – Technische Universität München, Germany.

[A55] Jean-Guillaume Dumas et Aude Rondepierre. – Modeling the electrical activity of a neuron by a continuous and piecewise affine hybrid system. Dans : **HSCC'2003, Proceedings of the 2003 Hybrid Systems : Computation and Control, Prague, The Czech Republic**, Oded Maler et Amir Pnueli éd., 3–5 avril 2003. – *LNCS*, volume 2623, pages 156–171. – Springer.

[A56] Jean-Guillaume Dumas, Thierry Gautier, Mark Giesbrecht, Pascal Giorgi, Bradford Hovinen, Erich Kaltofen, B. David Saunders, Will J. Turner et Gilles Villard. – LinBox: A generic library for exact linear algebra. Dans : **ICMS'2002, Proceedings of the 2002 International Congress of Mathematical Software, Beijing, China**, Arjeh M. Cohen, Xiao-Shan Gao et Nobuki Takayama éd., 17–19 août 2002. Pages 40–50. – World Scientific Pub.

[A57] Jean-Guillaume Dumas et Gilles Villard. – Computing the rank of sparse matrices over finite fields. Dans : **CASC'2002, Proceedings of the fifth International Workshop on Computer Algebra in Scientific Computing, Yalta, Ukraine**, Victor G. Ganzha, Ernst W. Mayr et

Evgenii V. Vorozhtsov éd., 22–27 septembre 2002. Pages 47–62. – Technische Universität München, Germany.

[A58] Jean-Guillaume Dumas et Jean-Louis Roch. – A fast parallel block algorithm for exact triangularization of rectangular matrices. Dans : **SPAA'01. Proceedings of the Thirteenth ACM Symposium on Parallel Algorithms and Architectures, Kreta, Greece**, Pierre Fraigniaud éd., 4–6 juillet 2001, pages 324–325.

## Conférences nationales avec comité de lecture et actes publiés

[B59] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici et Damien Pous. – Formal verification in Coq of program properties involving the global state effect. Dans : **JFLA 2014 : 25e Journées Francophones des Langages Applicatifs, Fréjus**, Christine Tasson éd., 8–11 janvier 2014, pages 1–15.

[B60] Jean-Guillaume Dumas et Dominique Duval. – Towards a diagrammatic modeling of the LinBox C++ linear algebra library. Dans : **LMO'2006, Langages et Modèles à Objets, Nîmes, France**, Roger Rousseau, Christelle Urtado et Sylvain Vauttier éd., 22–24 mars 2006. Pages 117–132. – Hermès.

[B61] Jean-Guillaume Dumas. – Calcul parallèle du polynôme minimal entier en Athapascan-1 et LinBox. Dans : **RenPar'2000. Actes des douzièmes rencontres francophones du parallélisme, Besançon, France**, Herv'e Guyennet éd., 19-22 juin 2000. – *TSI, Technique et science informatiques*, volume 20, pages 119–124. – Hermès sciences, Paris.

## Conférences internationales invitées avec actes publiés

[B62] Jean-Guillaume Dumas, Thierry Gautier, Clément Pernet et B. David Saunders. – LinBox founding scope allocation, parallel building blocks, and separate compilation. Dans : **ICMS'2010, Proceedings of the 2010 International Congress of Mathematical Software, Kobe, Japan**, Komei Fukuda, Joris vander Hoeven, Michael Joswig et Nobuki Takayama éd., 13–17 septembre 2010. – *LNCS*, volume 6327, pages 77–83. – Springer.

[B63] Jean-Guillaume Dumas, Clément Pernet et Jean-Louis Roch. – Adaptive triangular system solving. Dans : **Challenges in Symbolic Computation Software**, Wolfram Decker, Mike Dewar, Erich Kaltofen et Stephen M. Watt éd., 2–7 octobre 2006. Pages 1–18. – Dagstuhl Seminar proceedings 06271.

## Monographies

[L64] Jean-Guillaume Dumas, Pascal Lafourcade et Patrick Redon. – ***Architectures PKI et communications sécurisées***. – Dunod, 2015, 398 pages.

[L65] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Foundations of Coding: Compression, Encryption, Error-Correction***. – Wiley, USA, février 2015, 373 pages.

[L66] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Théorie des codes : compression, cryptage, correction***. – Dunod, 2013, $2^{e}$ édition, 384 pages.

[L67] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Théorie des codes : compression, cryptage, correction***. – Dunod, 2007, 352 pages.

## Chapitres de livres

[L68] Jean-Guillaume Dumas et Pascal Lafourcade. – Les crypto-monnaies, une réalité virtuelle ? Dans : **Les Big Data à découvert**, Mokrane Bouzeghoub et Rémy Mosseri éd., pages 298–299. – CNRS, mars 2017.

[L69] Jean-Guillaume Dumas et Clément Pernet. – Computational linear algebra over finite fields. Dans : **Handbook of Finite Fields**, Daniel Panario et Gary L. Mullen éd., pages 514–528. – Chapman & Hall/CRC, 2013.

[L70] Pascal Bouvry, Jean-Guillaume Dumas, Roland Gillard, Jean-Louis Roch et Sébastien Varrette. – Cryptographie à clef secrète. Dans : **Cryptographie et sécurité des systèmes et réseaux**, T. Ebrahimi, F. Leprevost et B. Warusfeld éd., pages 23–102. – Hermès, 2006.

[L71] Jean-Guillaume Dumas, Franck Leprevost, Jean-Louis Roch, Valentin Savin et Sébastien Varrette. – Cryptographie à clef publique. Dans : **Cryptographie et sécurité des systèmes et réseaux**, T. Ebrahimi, F. Leprevost et B. Warusfeld éd., pages 103–186. – Hermès, 2006.

[L72] Jean-Guillaume Dumas, Franck Leprevost, Jean-Louis Roch et Sébastien Varrette. – Architectures PKI. Dans : **Cryptographie et sécurité des systèmes et réseaux**, T. Ebrahimi, F. Leprevost et B. Warusfeld éd., pages 187–210. – Hermès, 2006.

[L73] Jean-Guillaume Dumas, Frank Heckenbach, B. David Saunders et Volkmar Welker. – Computing simplicial homology based on efficient Smith normal form algorithms. Dans : **Algebra, Geometry and Software Systems**, Michael Joswig et Nobuki Takayama éd., pages 177–206. – Springer, 2003.

## Actes de conférences

[L74] Jean-Guillaume Dumas et Erich Kaltofen (éditeurs). – ***PASCO'15, proceedings of the 5th acm international workshop on parallel symbolic computation, Bath, UK***, 10–11 juillet 2015. – ACM Press, New York.

[L75] Delphine Boucher, Thomas Cluzeau, Jean-Guillaume Dumas, et Grégoire Lecerf (éditeurs). – ***Journées nationales de calcul formel***, 3–7 mai 2010. – Centre de diffusion de revues académiques mathématiques.

[L76] Jean-Guillaume Dumas (éditeur). – ***ISSAC'2006, proceedings of the 2006acm international symposium on symbolic and algebraic computation, Genova, Italy***, 9–12 juillet 2006. – ACM Press, New York.

[L77] Jean-Guillaume Dumas (éditeur). – ***TC'2006, proceedings of transgressive computing 2006, Granada, España***, 24–26 avril 2006. – Universidad de Granada, Spain.

## Projets Internationaux

[P78] Projets INRIA Salsa, Arénaire (y compris L. J. Kuntzmann) et North Carolina State University. – QOLAPS : ***Quantifier Elimination, Optimization, Linear Algebra and Polynomial Systems***. – 15 k€/an, Équipe Associée INRIA-NSF, 2012-2015.

[P79] U. de Strasbourg, Tsinghua U. et U. de Grenoble. – FCSDH : ***Laboratoire Franco-Chinois sur les systèmes dynamiques hybrides***. – 16 k€, CNRS, 2002-2006.

## Projets Européens

[P80] Jacobs U. Bremen, Logilab, Simula Research Lab., U. Kaiserslautern, U. Sheffield, U. Silesia, U. Southampton, U. St Andrews, U. Warwick, U. Zurich, U. J. Fourier Grenoble, U. Paris-Sud, U. Bordeaux et U. Versailles. – OpenDreamKit : ***Open Digital Research Environment Toolkit for the Advancement of Mathematics***. – 7.6 M€, Horizon 2020 European Research Infrastructure project, 676541, 2015-2019.

[P81] L. J. Kuntzmann. – CC : ***Contrôle Hybride***. Dans : **Computation and Control**. – 4 k€, Projet Européen, 2003-2004.

Projets ANR

[P82] L. J. Kuntzmann, L. d'Informatique de Paris 6, L. Informatique de Grenoble, Laboratoire de l'Informatique du Parallélisme, L. d'Informatique, de Robotique et de Microélectronique de Montpellier et HPCProject. – HPAC : ***High Performance Algebraic Computations***. – 639 k€, ANR, ANR-11-BS02-013, 2012-2015.

[P83] L. d'Informatique de Paris Nord, L. Informatique de Grenoble, É. N. Supérieure des Télécommunications de Bretagne, Institut Fourier et L. J. Kuntzmann. – SAFESCALE : ***Certification et tolérance aux fautes sur grille de calcul***. – 120 k€, ANR, 2006-2009.

Projets Industriels

[P84] @GP. – CRYPTAAPKI : ***Formation Cryptographie asymétrique et architectures de sécurité***. – 5 k€, Contrat industriel, 2016.

[P85] Tiempo-Secure. – SIDERSA : ***Formation Attaques par perturbation sur RSA embarqué***. – 6 k€, Contrat industriel, 2015.

[P86] L. Informatique de Grenoble, Verimag, L. Jean Kuntzmann, Institut Fourier, Atos et SecLab. – ARAMIS : ***Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles***. – 820 k€, Investissements d'Avenir, 2014-2018.

[P87] L. Informatique de Grenoble, Verimag, L. Jean Kuntzmann, Institut Fourier, Communication & Systems, Netheos, iWall/Mataru et EasyiiC. – SHIVA : ***Secured Hardware Immune Versatile Architecture***. – 2.2 M€, Ministère de l'industrie, 2009-2011.

[P88] Communication & Systems, L. Informatique de Grenoble, L. J. Kuntzmann, Institut Fourier et Verimag. – EAU : ***Formations à la cryptologie et à la sécurité, mise en place d'infrastructures sécurisées.*** – 3 M€, Contrat industriel, 2006-2010.

Projets CNRS

[P89] L. Informatique de Grenoble, L. d'Informatique, Robotique, Micro-électronique de Montpellier, L. J. Kuntzmann et L. d'Informatique et du Parallélisme. – //INBOX : ***Outils logiciels pour le calcul algébrique haute performance***. – 12 k€, CNRS-PEPS, 2010-2012.

[P90] L. J. Kuntzmann. – SQUASH : ***Analyse qualitative des systèmes hybrides***. – 10 k€, CNRS, 2002-2003.

Projets Régionaux

[P91] L. J. Kuntzmann. – CHPID : ***Nouveaux outils mathématiques pour le calcul scientifique***. Dans : **Calcul Hautes Performances et Informatique Distribuée**. – 14 k€, Cluster ISLE de la Région Rhône-Alpes, 2005-2008.

[P92] L. J. Kuntzmann et L. d'InfoRmatique en Image et Systèmes d'information. – CALCEL : ***Calcul Cellulaire***. – 120 k€, Région Rhône-Alpes, 2005-2008.

Projets Université Grenoble Alpes

[P93] L. J. Kuntzmann et Institut Fourier. – MPLLC : ***Multi-Precision Library for Lattices and Cryptography***. – 55 k€, UJF-Pôle MSTIC, 2011-2012.

[P94] L. J. Kuntzmann. – CARESSE : ***Contrôle et Analyse de Réseaux de Systèmes Dynamiques Évolutifs***. – 65 k€, UJF-Pôle MSTIC, 2008-2009.

[P95] L. J. Kuntzmann et Institut Fourier. – PALO-ALTO : ***Plate-forme d'Attaques LOgicielles par ALgorithmes et Techniques Optimisés pour architectures Multi-Cœurs Parallèles***. – 57 k€, UJF-Pôle MSTIC, 2008-2009.

[P96] L. J. Kuntzmann et L. Informatique de Grenoble. – AHA : ***Algorithmes Hybrides Adaptatifs***. – 80 k€, IMAG, 2005-2007.

[P97] L. J. Kuntzmann et L. Logiciels Systèmes Réseaux. – INCA : ***Interfaces pour le calcul formel***. – 30 k€, IMAG, 2003-2004.

---

Logiciels (cf. `http://ljk.imag.fr/CASYS/LOGICIELS`)

---

[S98] Jean-Guillaume Dumas et Burak Ekici. – CoqEffects: Certified proofs in programs involving side-effects, 2013. 28 kSLOC.

[S99] Brice Boyer, Thierry Gautier, Gilles Villard, Jean-Louis Roch, Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – Givaro-3.7.0, a C++ library for computer algebra: exact arithmetic and data structures. – Debian (`libgivaro1, libgivaro-dev`), juin 2012. 48 kSLOC.

[S100] The LINBOX group. – LINBOX 1.3.0. – Debian (`liblinbox0, liblinbox-dev`), mai 2012. 213 kSLOC.

[S101] Brice Boyer et Jean-Guillaume Dumas. – FFSpMv: Finite field sparse matrix-vector product on multi-cores, 2010. 43 kSLOC.

[S102] Brice Boyer et Jean-Guillaume Dumas. – Galet: Matrix multiplication schedule generator, janvier 2009. 11 kSLOC.

[S103] Jean-Guillaume Dumas et Clément Pernet. – Exact linear system resolution in M4RI, novembre 2008.

[S104] Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi et Clément Pernet. – FFLAS-FFPACK: Finite field linear algebra subroutine/package, février 2006. 21 kSLOC.

[S105] Aude Rondepierre et Jean-Guillaume Dumas. – Hybrid optimal control, 2005. 7 kSLOC.

[S106] Jean-Guillaume Dumas, Frank Heckenbach, B. David Saunders et Volkmar Welker. – ***Simplicial homology, a (proposed) share package for gap***, mars 2000. Manual.

---

Rapports de recherche et prépublications soumises

---

[T107] Jean-Guillaume Dumas, Erich Kaltofen et Emmanuel Thomé. – ***Interactive certificate for the verification of Wiedemann's Krylov sequence: application to the certification of the determinant, the minimal and the characteristic polynomials of sparse matrices***. – Rapport technique, IMAG-hal-01171249 arXiv cs.SC/1507.01083, janvier 2016.

[T108] Jean-Guillaume Dumas et Victor Y. Pan. – ***Fast matrix multiplication and symbolic computation***. – Rapport technique, IMAG-hal-01417524 arXiv cs.SC/1612.05766, décembre 2016.

[T109] Jean-Guillaume Dumas. – ***Contributions au calcul exact intensif***. – Habilitation à diriger des recherches en Informatique et mathématiques appliquées, Université de Grenoble, 20 juillet 2010.

[T110] Jean-Guillaume Dumas. – ***Algorithmes parallèles efficaces pour le calcul formel : algèbre linéaire creuse et extensions algébriques***. – Thèse de Doctorat en mathématiques appliquées, Institut National Polytechnique de Grenoble, France et University of Delaware, USA, 20 décembre 2000.

---

Co-auteurs

---

1. Benoît Badrignans ; 2. Alexandre Berzati ; 3. Pascal Bouvry ; 4. Brice Boyer ; 5. Alexis Breust ; 6. Xavier Bultel ; 7. Christophe Chabot ; 8. Van-Dat Cung ; 9. Vincent Danjean ; 10. Jannik Dreier ; 11. Jacques Dubrois ; 12. Cécile Dumas-Canovas ; 13. Dominique Duval ; 14. Burak Ekici ; 15. Philippe Elbaz-Vincent ; 16. Laurent Fousse ; 17. Thierry Gautier ; 18. Mark W. Giesbrecht ; 19. Roland Gillard ; 20. Pascal Giorgi ; 21. Louis Goubin ; 22. Rod Gow ; 23. Frank Heckenbach ; 24. Hicham Hossayni ; 25. Bradford Hovinen ; 26. Guillaume Huard ; 27. Hugo Jonker ; 28. Erich L. Kaltofen ; 29. Pascal Lafourcade ; 30. Franck Leprévost ; 31. David Lucas ; 32. Sabine Machenaud ; 33. Gary McGuire ; 34. Francis Melemedjian ; 35. Gregory Nuel ; 36. Jean-Baptiste Orfila ; 37. Clément Pernet ; 38. Victor Y. Pan ; 39. Florian Pebay-Peyroula ; 40. François Pebay-Peyroula ; 41. Marie-Laure Potet ; 42. Damien Pous ; 43. Maxime Puys ; 44. Bruno Raffin ; 45. Christophe Rapine ; 46. Patrick Redon ; 47. Jean-Claude Reynaud ; 48. Jean-Luc Richier ; 49. Jean-Louis Roch ; 50. Aude Rondepierre ; 51. Bruno Salvy ; 52. B. David Saunders ; 53. Valentin Savin ; 54. John Sheekey ; 55. Ziad Sultan ; 56. Éric Tannier ; 57. Emmanuel Thomé ; 58. Pascal Thoniel ; 59. Denis Trystram ; 60. Will J. Turner ; 61. Anna Urbańska ; 62. Sébastien Varrette ; 63. Gilles Villard ; 64. Zhendong Wan ; 65. Volkmar Welker ; 66. Lihong Zhi ; 67. Wei Zhou ; 68. Vincent Zucca.

## RÉFÉRENCES


[111 - Gao (2016)] Xiao-Shan Gao (éditeur). – ***ISSAC'2016, proceedings of the 2016 acm international symposium on symbolic and algebraic computation, Waterloo, Canada***, 20–22 juillet 2016. – ACM Press, New York.

[112 - Gutierrez (2004)] Jaime Gutierrez (éditeur). – ***ISSAC'2004, proceedings of the 2004acm international symposium on symbolic and algebraic computation, Santander, Spain***, 4–7 juillet 2004. – ACM Press, New York.

[113 - Jeffrey (2008)] David Jeffrey (éditeur). – ***ISSAC'2008, proceedings of the 2008acm international symposium on symbolic and algebraic computation, Hagenberg, Austria***, 20–23 juillet 2008. – ACM Press, New York.

[114 - Kauers (2005)] Manuel Kauers (éditeur). – ***ISSAC'2005, proceedings of the 2005acm international symposium on symbolic and algebraic computation, Beijing, China***, 24–27 juillet 2005. – ACM Press, New York.

[115 - Kauers (2013)] Manuel Kauers (éditeur). – ***ISSAC'2013, proceedings of the 2013acm international symposium on symbolic and algebraic computation, Boston, USA***, 26–29 juin 2013. – ACM Press, New York.

[116 - May (2009)] John P. May (éditeur). – ***ISSAC'2009, proceedings of the 2009acm international symposium on symbolic and algebraic computation, Seoul, Korea***, 28–31 juillet 2009. – ACM Press, New York.

[117 - Mora (2002)] Teo Mora (éditeur). – ***ISSAC'2002, proceedings of the 2002acm international symposium on symbolic and algebraic computation, Lille, France***, 7–10 juillet 2002. – ACM Press, New York.

[118 - Moreno-Maza et Roch (2010)] Marc Moreno-Maza et Jean-Louis Roch (éditeurs). – ***PASCO'10, proceedings of the 4th acm international workshop on parallel symbolic computation***, 21–23 juillet 2010. – Université de Grenoble, France.

[119 - Nabeshima (2014)] Katsusuke Nabeshima (éditeur). – ***ISSAC'2014, proceedings of the 2014acm international symposium on symbolic and algebraic computation, Kobe, Japan***, 23–25 juillet 2014. – ACM Press, New York.

[120 - Safey El Din (2017)] Mohab Safey El Din (éditeur). – ***ISSAC'2017, proceedings of the 2017 acm international symposium on symbolic and algebraic computation, Kaiserslautern, Deutschland***, 25–28 juillet 2017. – ACM Press, New York.

[121 - Traverso (2000)] Carlo Traverso (éditeur). – ***ISSAC'2000, proceedings of the 2000acm international symposium on symbolic and algebraic computation, Saint-Andrews, Scotland***, 6–9 août 2000. – ACM Press, New York.

[122 - Yokoyama (2015)] Kazuhiro Yokoyama (éditeur). – ***ISSAC'2015, proceedings of the 2015acm international symposium on symbolic and algebraic computation, Bath, UK***, 6–10 juillet 2015. – ACM Press, New York.