JEAN-GUILLAUME DUMAS

10 SEPTEMBRE 2021

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

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

700 avenue centrale,
IMAG CS-40700, bur. 115,
38058 Grenoble, France.
Tél. : 33 (0) 457 421 732

Parcours professionnel et formation

Depuis 2021 : **Directeur**, *Laboratoire Jean Kuntzmann*, umr 5224.

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

2020 : Directeur adjoint, puis directeur par interim, *Laboratoire Jean Kuntzmann*.

2016-2020 : Responsable du master CyberSecurity, UFR IM^{2}AG et Grenoble INP.

2017-2020 : Équipe CAS^{3}C^3 du LJK, responsable.

2018-2019 : Cryptography Advisor, ConsenSys corp.

2014-2016 : Responsable du département modèles et algorithmes déterministes au LJK.

2015-2019 : Projet européen OPENDREAMKIT.

2013-2017 : ACM SIGSAM, vice chair.

2015-2017 : ACM PASCO steering committee chair.

Automne 2015 : Semestre invité, Fields Institute, Toronto, Canada.

2012-2016 : Projet ANR HPAC (high-performance algebraic computing), coordinateur.

2011-2015 : Master 1 Mathématiques Appliquées et Industrielles, UFR IM^{2}AG, responsable.

Juillet 2010 : HDR de l'*Université de Grenoble* : contributions au calcul exact intensif.

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

2006-2009 : Équipe CASYS du LJK, responsable.

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

2000-2002 : ATER *ENSIMAG*.

1997-2000 : Doctorat de l'*INPG* au *laboratoire Informatique & Distribution* et à l'*université du Delaware*, USA : Algorithmes parallèles efficaces pour le calcul formel.

Encadrement d'activités de recherche

Thèses en cours

2. Thèse CyberSecurity Institute : **Florentina Șoiman** (directrice S. Jimenez Garces) : *Blockchain and smart contracts: Benefits and risks for financial markets and institutions*. Depuis septembre 2019.

1. Thèse MESR **Nicolas Bordes** (co-directeurs P. Karpman & P. Maistri) : *Symmetric primitives of low multiplicative complexity, side-channel attacks and masking*. Depuis octobre 2018.

8 Docteurs : **David Lucas** (directeur C. Pernet) : *Secure and efficient outsourced computation protocols for linear algebra*, 2020. **Jean-Baptiste Orfila** : *Architecture de sécurité et protocoles cryptographiques pour les systèmes de contrôle-commande*, 2018 ; **Ziad Sultan**, projet ANR-11-BS02-013 HPAC (co-directeur C. Pernet) : *Parallel building blocks for high-performance algebraic computations*, 2016 ; **Burak Ekici** (co-directrice D. Duval) : *Certification de programmes avec des effets calculatoires*, 2015 ; **Brice Boyer** : *Multiplication matricielle efficace et conception logicielle pour la bibliothèque de calcul exact* LINBOX, 2012 ; **Anna Urbańska** (directrice D. Duval) : *Hybrid and adaptive algorithms in exact linear algebra*, 2010 ; **Clément Pernet** (directrice D. Duval) : *Algèbre linéaire exacte efficace : le calcul du polynôme caractéristique*, 2006 ; **Aude Rondepierre** (directeur J. Della Dora) : *Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires*, 2006.

5 Post-doctorants et ingénieurs de recherche : **Alexis Breust** : *Certificats de preuves de travail en algèbre linéaire exacte*, 2018-2019 ; **Zhu Hong Guang** : *Exact linear algebra routines over distributed memory plateforms and GPU*, 2017-2019 ; **Alexis Breust** : *Routines d'arithmétique exacte à précision arbitraire*, 2014-2015 ; **Guillaume Ollier** : *Problèmes LWE et Ring-LWE : liens avec les réseaux, difficultés et implémentations pratiques*, 2011-2012 ; **Christophe Chabot** : *Entiers récursifs à précision fixée sur FPGA*, 2010-2011.

Ceci s'ajoute à la direction de 15 Master 2 Recherche et une quarantaine de TER Master 1 (en Informatique, en Mathématiques et en Mathématiques Appliquées à l'UGA et à l'ENSIMAG).

Collaborations au sein de projets académiques et industriels

Ma recherche s'est également concrétisée à travers 23 projets de recherche académiques et industriels (2 Internationaux, 2 Européens, 2 ANR, 7 FUI/PIA, 2 CNRS, 2 Régionaux, 6 Université de Grenoble), dans les thèmes suivants : Conception et modélisation logicielles ; Cryptologie, codes, arithmétique ; calcul algébrique intensif ; Systèmes dynamiques hybrides symboliques-numériques.

Publications

100 Publications
(accessibles sur : membres-ljk.imag.fr/Jean-Guillaume.Dumas/publications.html) :

- 17 ISSAC (conférence internationale majeure du calcul formel).
- 23 Revues internationales : J. Symbolic Computation ; Computers & Security ; Theoretical Computer Science ; Lin. Alg. & Appl. ; Finite Fields & Appl. ; J. Computer Security ; ACM Trans. on Math. Software ; IEEE Trans. on Computers ; Inf. Proc. Letters ; Parallel Computing ; Math. Struc. in Comp. Science ; J. of Inequalities in Pure and Applied Mathematics ; Math. & Sciences Humaines.
- 37 Autres conférences internationales à comité de lecture et actes publiés.
- 14 Monographies et chapitres de livres.
- 9 Logiciels.

93 Communications, séminaires et séjours de recherche nationaux et internationaux (notamment à SIAM LA2021, WFC2021, CCS 2019, HistCalc 2019, CASC 2018, MICA 2016, RESSI 2016, LCASNC 2015, OZSSI 2015, SDTA 2014, ISSAC 2014 / 2005, PMAA 2014, SIAM PP 2014, JNCF 2020 / 2014 / 2007 / 2005, ILAS 2013, HotSpot 2013, SIAM AG 2011, ICMS 2010 / 2006, IWCL 2010, CSIWCC 2010, WCS 2009, CAT 2009, ACA 2009 / 2002, ACCAT 2009, CCS-IC 2009, CLPASCS 2005, HSCC 2002, etc).

Quelques publications récentes, caractéristiques des domaines de spécialité :

— Dynamic proofs of retrievability with low server storage avec Gaspard Anthoine, Michael Hanling, MÃ©lanie de Jonghe, Aude Maignan, Clément Pernet, et Daniel S. Roche. 30th USENIX Security Symposium, pages 537–554, 11–13 Août 2021.

— Elimination-based certificates for triangular equivalence and rank profiles avec Erich L. Kaltofen, Clément Pernet et David Lucas. Journal of Symbolic Computation. Volume 98, pages 246–269, Mai-Juin 2020.

— A Faster Cryptographer's Conspiracy Santa avec Xavier Bultel, Jannik Dreier et Pascal Lafourcade. Theoretical Computer Science. vol. 839, pages 122–134, Nov. 2020.

— LU factorization with errors avec Joris van der Hoeven, Clément Pernet et Daniel S. Roche. ISSAC 2019, pages 131–138, Beijing, Chine, 15–18 Juillet 2019.

— Proof-of-work certificates that can be efficiently computed in the cloud. Lecture Notes in Computer Science, vol. 11077, pages 1–17, Sep. 2018.

— Polynomial Time Interactive Proofs for Linear Algebra with Exponential Matrix Dimensions and Scalars Given by Polynomial Time Circuits, avec Erich Kaltofen, Gilles Villard et Lihong Zhi. ISSAC 2017, pages 125–132, Kaiserslautern, Deutschland, 25–28 Juillet 2017.

— Dual protocols for private multi-party matrix multiplication and trust computations avec Pascal Lafourcade, Jean-Baptiste Orfila et Maxime Puys. Computers & Security. Volume 71, pages 51–70, Nov. 2017.

— Recursion based parallelization of exact dense linear algebra routines for Gaussian elimination avec Thierry Gautier, Clément Pernet, Jean-Louis Roch et Ziad Sultan. Parallel Computing, Volume 57, pages 235–249, Septembre 2016.

Prix, distinctions

- *Étoile de l'Europe, mention science ouverte* pour le projet OpenDreamKit, 2020.
- *Best Paper Award*, SECRYPT 2016.
- ACM SIGSAM *Distinguished Paper Award*, ISSAC 2015.
- Titulaire de la PEDR 2005-2009, 2009-2013 (PES), 2014-2018, 2018-2022.
- Accessit au concours général de mathématiques 1992.

Enseignements

Environ 200h/an :

— Cryptologie ; codes correcteurs ; compression ; arithmétique.

— Calcul scientifique ; Calcul formel.

— Langages de programmation ; Système ; Algorithmique ; Parallélisme.

— Sécurité Web/Réseaux ; PKI ; Architectures de sécurité.

— Algèbre ; Analyse.

Rayonnement

Éditeur associé des journaux *ACM Communications in Computer Algebra*, depuis 2006 ; *Maple Transactions*, depuis 2021.

16 Organisations de conférences.

23 Expertises nationales et internationales (American U. of Beirut, FWF Autriche, Inria, AERES, ANR, INFORMS-USA, NSA-AMS-USA, NSER-Canada, Agence Tchèque de subventions), etc.

3 Comités scientifiques nationaux et internationaux (SIGSAM, JNCF, ILAS).

25 Jurys de thèses et HDR.

103 Comités de lecture ou de programmes.