CURRICULUM VITÆ

16 AVRIL 2025

Jean-Guillaume Dumas

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

ANIMATION SCIENTIFIQUE

Jean-Guillaume Dumas, 50 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

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

Parcours professionnel et formation

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

Depuis 2020 : **Directeur**, Laboratoire Jean Kuntzmann (LJK), umr UGA/CNRS 5224.

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

2017-2020 : **Responsable de l'équipe** CAS^{3}C^3 du LJK.

2018-2019 : **Cryptography Advisor**, ConsenSys corp.

2014-2016 : **Responsable de département** MAD (modèles et algorithmes déterministes), *laboratoire Jean Kuntzmann*.

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.

2006-2009 : **Responsable de l'équipe** CASYS du LJK.

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

1. Thèse UGA : **Alexis Galan** (co-directeur·rice·s B. Grenet & A. Maignan) : *Protection of Whistleblowers and Private Operations on Sets*. Depuis octobre 2023.

Thèses soutenues

10. Thèse CyberSecurity Institute : **Florentina Șoiman** (directrice S. Jimenez Garces) : *Risk-Return relationship. The case of Blockchain technology and the crypto-market*. Soutenue le 7 décembre 2022. F. Șoiman est **financial operations analyst**, IMC, Rotterdam, Pays-Bas.

9. Thèse MESR : **Nicolas Bordes** (co-directeurs P. Karpman & P. Maistri) : *Symmetric primitives of low multiplicative complexity, side-channel attacks and masking*. Soutenue le 9 décembre 2021. N. Bordes est **ingénieur** cybersécurité, Ledger, Paris.
8. Thèse H2020-OpenDreamKit : **David Lucas** (directeur C. Pernet) : *Secure and efficient outsourced computation protocols for linear algebra*. Soutenue le 10 juillet 2020. D. Lucas est **ingénieur en sécurité applicative**, Strasbourg.
7. Thèse PIA-Aramis **Jean-Baptiste Orfila** : *Architecture de sécurité et protocoles cryptographiques pour les systèmes de contrôle-commande*. Soutenue le 10 juillet 2018. J-B. Orfila est **ingénieur R&D** en cybersécurité, Zama, Paris.
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 **ingénieur R&D** calcul haute-performance, 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 **associate professor**, Université de Mugla, Turquie.
4. Thèse MESR **Brice Boyer** : *Multiplication matricielle efficace et conception logicielle pour la bibliothèque de calcul exact* LinBox. Soutenue le 21 juin 2012. B. Boyer est **ingénieur**, Paris.
3. Thèse MESR **Anna Urbańska** (directrice D. Duval) : *Hybrid and adaptive algorithms in exact linear algebra*. Soutenue le 27 avril 2010. A. Urbańska est ensuite devenue **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. C. Pernet est **professeur des universités** à l'Ensimag, Grenoble.
1. Thèse MESR **Aude Rondepierre** (directeur J. Della Dora) : *Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires*. Soutenue le 18 juillet 2006. A. Rondepierre est **professeure des universités** à l'INSA et à l'institut de mathématiques de Toulouse.

Post-doctorants et ingénieurs de recherche

6. Ingénieur de recherche, projet Notare SigNum **Anthony Craignic** : *Architecture de Sécurité pour certifications locales et signatures juridiques*, 2024-2026.
5. Ingénieur de recherche, projet OpenDreamKit **Alexis Breust** : *Certificats de preuves de travail en algèbre linéaire exacte*, 2018-2019.
4. Ingénieur de recherche, projet OpenDreamKit **Zhu Hong Guang** : *Exact linear algebra routines over distributed memory plateforms and GPU*, 2017-2019.
3. Ingénieur de recherche, projet Hpac **Alexis Breust** : *Routines d'arithmétique exacte à précision arbitraire*, 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 **18 Master-2 Recherche** : A. Rondepierre (2002), C. Pernet et P. Vignard (2003), J. Dubrois et I. Hatm (2004), B. Boyer (2008), A. Al Rashedi (2009), H. Hossayni (2011), J-B. Orfila (2014), V. Zucca (2015), A. Bouguera (2016), H. Mertzweiller (2018), L. Robert (2019), G. Anthoine et L. Assekour (2021), A. Martinez (2022), A. Galan (2023) et L. Barros Reis Soezima (2025).

Participation à plus d'une centaine de jurys de DEA/Master 2 (notamment récemment pour le Master Cybersecurity).

Direction de **50 TER Master-1 et tutorats d'alternance** (en Informatique, en Mathématiques et en Mathématiques Appliquées à l'UGA et à l'ENSIMAG) : 3*2003, 4*2004, 2*2005, 2*2006, 7*2007, 5*2008, 2009, 2011, 2*2012, 6*2013, 2014, 2015, 2*2016, 2*2017, 3*2018, 2019, 2*2020, 2021, 2022, 2023, 2024, 2025.

Jurys de thèse et d'HDR

33. **Guilhèm Assael** (président), U. Grenoble Alpes : *Accélération matérielle de cryptographie post-quantique pour les systèmes embarqués*, décembre 2024.
32. **Gael Marcadet** (président), U. Clermont Auvergne : *Design of Secure Multi-Users Protocols, Applications to Bandits, Ticketing and File Transfer*, juillet 2024.
31. **Remi Adelin** (rapporteur), INSA Toulouse : *Protection des données des véhicules connectés : une approche cryptographique reposant sur le chiffrement basé attributs*, juillet 2023.
30. **Florentina Șoiman** (co-directeur), U. Grenoble Alpes : *Blockchain and smart contracts: Benefits and risks for financial markets and institutions*, décembre 2022.
29. **Léo Robert** (examinateur), U. Clermont Auvergne : *Design and Verification of Security Protocols for Heterogeneous 5G IoT Devices*, septembre 2022.
28. **Mohamed Traoré** (président), U. Grenoble Alpes : *Analyse et contre-mesures des biais de RNG pour les mécanismes cryptographiques et applications industrielles*, avril 2022.
27. **Nagarjun Dwarakanath** (rapporteur), U. Paris-Saclay : *Contributions théoriques et pratiques au chiffrement homomorphe*, décembre 2021.
26. **Nicolas Bordes** (co-directeur), U. Grenoble Alpes : *Symmetric primitives of low multiplicative complexity, side-channel attacks and masking*. décembre 2021.
25. **Mirko Koscina** (président), ÉNS Paris : *Security and Optimization of Blockchains and Associated Algorithms*, octobre 2021.
24. **Jocelyn Ryckeghem** (rapporteur), Sorbonne U. : *Cryptographie Post-Quantique : Conception et Analyse en Cryptographie Multivariée*, février 2021.
23. **David Lucas** (co-directeur), U. Grenoble Alpes : *Secure and efficient outsourced computation protocols for linear algebra*, juillet 2020.
22. **Matthieu Giraud** (président), U. Clermont-Ferrand, *Cloud security: secure, verifiable and searchable computation*, septembre 2019.
21. **Christoph Lauter** (habilitation, président), Sorbonne U., *Arithmétique flottante sûre*, mai 2019.
20. **Claire Delaplace** (président), U. Rennes, *Algorithmes d'algèbre linéaire pour la cryptographie*, novembre 2018.
19. **Jean-Baptiste Orfila** (directeur), U. Grenoble Alpes, *Architecture de sécurité et protocoles cryptographiques pour les systèmes de contrôle-commande*, juillet 2018.
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, *Certification de programmes avec des effets calculatoires*, 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, *Études 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, *Multiplication matricielle efficace et conception logicielle pour la bibliothèque de calcul exact* LINBOX, 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, *Hybrid and adaptive algorithms in exact linear algebra*, avril 2010.
3. **Clément Pernet** (co-directeur), U. J. Fourier, Grenoble, *Algèbre linéaire exacte efficace : le calcul du polynôme caractéristique*, septembre 2006.
2. **Aude Rondepierre** (co-directeur), INP Grenoble, *Algorithmes hybrides pour le contrôle optimal des systèmes non linéaires*, juillet 2006.
1. **Éric Tannier** (examinateur), U. J. Fourier, Grenoble, *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 à Grenoble INP et maître de conférences UJF, et depuis 2012 en tant que professeur UGA.

Modules enseignés

Enseignement	Unité	Années	Niv.	Type	Nature	Eff.	Vol.
Security Architectures	UFR im^{2}ag	2016-	M2	FI	C/TD/TP	40	60h
Blockchains & Sécurité	UFR im^{2}ag	2019-	M2	App.	C	15	18h
Codes : crypto. & correction d'erreurs	Ensimag	2016-	M1	FI	C/TD	80	36h
Cryptographic engineering	UFR im^{2}ag	2016-18	M1	FI	C/TD/TP	25	40h
Introd. to cryptology and coding	MOSIG	2015-18	M1	FI	C/TD/TP	50	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
Trait. algébrique de l'information	Ensimag	2011-16	M1	FI	C/TD	40	36h
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'	1999-04	L3	FI	C/TD	80	32h
Algèbre	DSU UJF	1997-00	L1	FI	TD	40	32h
Analyse	DSU UJF	1997-00	L1	FI	TD	40	32h

TABLE 1 – Volume horaire annuel par module enseigné depuis 1997

Responsabilité de filière

Il y a quelques années, je m'étais largement investi dans le master 1 Mathématiques Appliquées et Industrielles. J'avais 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. Par la suite, j'ai pris en 2016, jusqu'en 2020, la responsabilité du Master 2 Cybersecurity, suite à l'évolution internationale du Master SCCI.

Développement à l'international et Master 2 Cybersecurity

Avec Jean-Louis Roch, nous avions été amenés, à travers plusieurs contrats de formation [P121, P118, P117, P116], à développer 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 international de Grenoble, CyberSecurity.
En effet, après mon doctorat, je me suis formé à l'enseignement en codes correcteurs, compression et cryptologie, et notamment après une année de visite d'un an au Claude Shannon Institute à Dublin. J'ai été impliqué par exemple dans la construction d'une grande partie 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). J'ai ensuite pris la responsabilité de cette filière, remaniée en Master 2 CyberSecurity, fin 2015 (plusieurs centaines de candidatures internationales par an, pour des promotions d'une quarantaine d'étudiants). J'ai également été impliqué dans le montage et le développement de la spécialité en apprentissage SAFE, Sécurité, Audit et Forensique pour l'Entreprise, en 2011, devenue le master Cybersecurite et Informatique legale (CSI) en 2017.

Supports d'enseignement en cryptologie, codes et cybersécurité

Avec le développement d'enseignements en calcul exact, en algorithmique de la théorie des nombres, en cryptologie, en compression de données, en correction d'erreur et en cybersécurité en général, j'ai rédigé plusieurs supports de cours dans ces domaines. Ceux-ci se sont ensuite concrétisés par la publication de plusieurs chapitres d'ouvrages de référence sur le sujet [L98, L99, L100, L96, L95] ainsi que plusieurs manuscrits à destination des Masters [L91, L90, L89, L87, L86, L85].

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

Cours Cryptomonnaies et NFT : mythes ou réalités ? CCI Îles de Guadeloupe, Octobre 2022.

Cours Les blockchains, des systèmes distribués. Parcours Innovateur, Ensimag, Grenoble, février 2020.

Cours La sécurité de Bitcoin et des blockchains. Parcours Innovateur, Ensimag, Grenoble, mai 2019.

Cours C++ haute-performance. Formation continue, Grenoble, novembre 2017.

Cours Architectures de sécurité. Formation continue, Montélier, juin 2016.

Cours Attaques par perturbation sur RSA embarqué. Formation continue, Montbonnot, juin 2015.

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

Le calcul scientifique est souvent associé au calcul numérique. Pourtant, dans de nombreuses disciplines scientifiques, il est nécessaire d'aller au-delà du calcul approché : instabilité des algorithmes numériques, nécessité de certification des résultats, calculs dans des structures mathématiques discrètes, notamment dans les domaines de la cryptologie, des codes et de la cybersécurité. Le calcul exact s'attache donc à donner des résultats exacts ou vérifiés et les défis sont multiples : développer des arithmétiques efficaces dans des structures discrètes ; concevoir des algorithmes haute performance même en tenant compte de la croissance des données intermédiaires ; transcrire ces algorithmes dans des logiciels combinant efficacité pérenne, interfaçage et généricité.
Notre approche consiste à produire des algorithmes et des logiciels génériques les plus efficaces possibles. En effet, deux stratégies extrêmes sont les plus fréquentes : développer un module spécifique à une application ou développer un système de calcul. Nous nous situons entre ces deux approches, au niveau parfois appelé intergiciel. Notre but est de fournir des routines quasiment aussi efficaces que des routines dédiées, mais avec un plus large spectre d'applications. En ce sens, les bibliothèques GIVARO et LINBOX, tout en étant des outils de recherche permettant de développer rapidement des solutions pour de nombreuses applications, ont également été choisies comme noyaux efficaces du système SAGE. Au niveau algorithmique, la difficulté est d'identifier les domaines d'applicabilité des différentes solutions existantes ou d'en créer de nouvelles. L'analyse de complexité joue alors un rôle prépondérant pour prévoir le comportement des différentes instances. Si parmi les nouveaux algorithmes proposés, certains améliorent l'exposant de complexité, une particularité de notre approche est de s'intéresser largement aux constantes et facteurs logarithmiques pour proposer plus généralement des algorithmes de meilleur *terme dominant* de complexité.
Au niveau thématique, j'ai d'abord effectué mon doctorat sur le **calcul haute performance**. J'ai ensuite travaillé en **calcul formel et systèmes dynamiques** en tant que maître de conférences. Ma recherche s'est ensuite largement tournée vers les **codes correcteurs**, notamment avec une délgation au Claude Shannon Institute à Dublin en 2009. Depuis six ans, ma recherche s'oriente de plus en plus vers la **cybersécurité**.

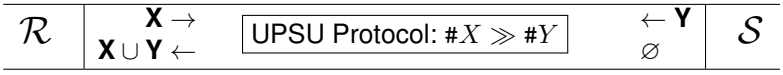
Calcul exact haute performance Le cœur de mon travail réside dans la réalisation efficace d'algorithmes exacts. L'analyse de complexité en temps et en mémoire est l'élément principal pour comparer les algorithmes et implémentations proposées à l'existant.
Cela induit de nombreux travaux sur l'algorithmique en algèbre linéaire ou polynomiale (Smith [A20, A43]; Kalman [A17, A75, A33]; Frobenius [B81, A16, A40, A14]; Bruhat, notamment depuis 2017, [A78, A42, A77, A73, B84, A12, A63, A10, A29, A28, A6, A4, A22, A3, T149]), des développements haute-performance sur accélérateurs et architectures hétérogènes [A76, A68, B83, A72, A19, A18, A71, A67, A39, A13, A74, A15, A70, A36, L97, A61, A57, A30, S139, S141, S138] et des conceptions et modélisations logicielles [S148, S147, B80, S144, A35, A34, S142, B79, A62, A60, A1, A2, S134, S135, T150].
Dans ce cadre, les développements se sont concrétisés par des collaborations de long terme avec plusieurs universités en France, au Canada et aux États-Unis (U. de Grenoble, ÉNS Lyon, U. de Montpellier, U. of Waterloo, U. of Calgary, U. of Delaware et North Carolina State U.).

Cybersécurité, calcul multi-parties, cryptologie Une partie importante de mon activité est dorénavant consacrée à des protocoles de cryptologie, de codes correcteurs ou de cybersécurité. Dans ce cadre nous nous intéressons particulièrement aux interactions et là encore à développer des techniques intermédiaires pour des classes de protocoles. Nous appliquons ceci pour par exemple définir des familles de codes à métrique de rang [A38, A37]; des attaques et implémentations embarquées [A69]; le développement d'algorithmes de cryptographie physique depuis 2016 [A58, A53, A51, A52, A24, A23]; et plus largement des travaux sur les architectures de sécurité [A66, A55, A54, A26, L87]; le calcul vérifiable depuis 2014 ou auto-correcteur depuis 2019 [A11, A9, A56, A8, A7, B82, A5, A25, L94] et les protocoles multi-partites sécurisés, notamment depuis 2016, [A64, A31, A59, A27, A50, A48, A47, A46] ou encore les blockchains et les actifs financiers associés depuis 2020 [L86, L85, A49, T151, A21]; avec en cybersécurité également un important développement de logiciels [A41, S146, S143, A32, S140, S136, S133].

Cinq publications récentes

1. Communication Optimal Unbalanced Private Set Union [A46], avec Alexis Galan, Bruno Grenet, Aude Maignan, et Daniel S. Roche. ACNS 2025: 23rd International Conference on Applied Cryptography and Network Security, Munich, Germany, 23–26 Juin 2025.

   Les protocoles privés sur les ensembles permettent à plusieurs parties de réaliser ensemble certaines fonctions de leurs ensembles respectifs sans révéler aux autres participants la totalité de leurs informations. Dans ce cadre, nous avons contruit le premier protocole privé d'union déséquilibrée d'ensembles (UPSU) n'utilisant que le volume de communication minimal pour cette tâche.



2. In-place accumulation of fast multiplication formulae [A1], avec Bruno Grenet. ISSAC 2024 : ACM International Symposium on Symbolic and Algebraic Computations, pages 16–25, Raleigh, NC USA, 16–19 Juillet 2024

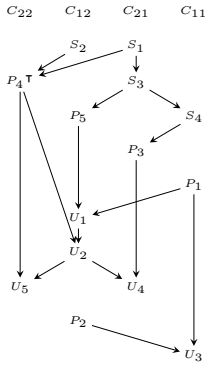
   Cet article traite d'algorithmes rapides et en place (n'utilisant que seuelement $O(1)$ espace supplémentaire) pour les formules dont le résultat doit être accumulé : certaines variables de sortie sont également des variables d'entrée, liées par une dépendance linéaire. La difficulté réside dans la combinaison de calculs en place et d'algorithmes rapides car ces derniers ont été généralement construit à l'aide d'un espace temporaire supplémentaire potentiellement important.

   Nous avons proposé une génération automatique d'algorithmes d'accumulation à la fois rapides et en place pour toute formule bilinéaire. Cela nous a permi de dériver des algorithmes sans précédent pour la multiplication polynomiale rapide et pour la multiplication matricielle rapide.

$$\left[R\right] = \sum_{i=0}^{\mu} \left[-GT^{-1}\right]^{i} \cdot \left[A_i\right]$$

3. Some fast algorithms multiplying a matrix by its adjoint [A22], avec Clément Pernet et Alexandre Sedoglavic. Journal of Symbolic Computation. Volume 115, pages 285–315, Mars-Avril 2023.

$YY^{\intercal}=-I,\ S_1\leftarrow(A_{21}-A_{11})Y;\ S_2\leftarrow A_{22}-A_{21}Y;$
$S_3\leftarrow S_1-A_{22};\quad S_4\leftarrow S_3+A_{12};\quad P_1\leftarrow A_{11}A_{11}{}^{\intercal};$
$P_2\leftarrow A_{12}A_{12}{}^{\intercal};\quad P_3\leftarrow A_{22}S_4{}^{\intercal};\quad P_4\leftarrow S_1S_2{}^{\intercal};$
$P_5\leftarrow S_3S_3{}^{\intercal};\quad U_1\leftarrow P_1+P_5;\quad U_2\leftarrow U_1+P_4;$
$C_{11}\leftarrow P_1+P_2;C_{21}\leftarrow U_2+P_3;C_{22}\leftarrow U_2+P_4{}^{\intercal}.$

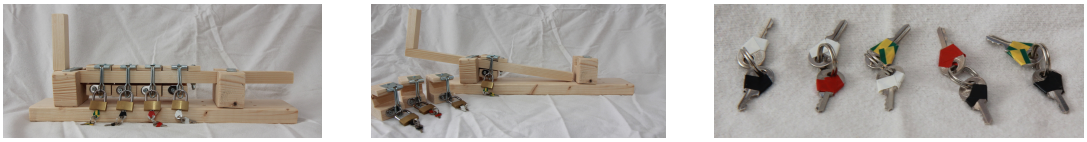


   Nous avons découvert récemment un nouvel algorithme de multiplication par blocs d'une matrice par sa transposée (ou son adjoint). L'algorithme utilise seulement 5 produits de blocs (au lieu de 6, voir ci-contre l'ordonnancement en place) sur les complexes ou sur tout corps de caractéristique non nulle. Cet algorithme découle de considérations géométriques sur l'espace des formes bilinéaires associées et améliore d'un facteur constant les précédentes réductions connues. La géométrie nous permet en outre d'obtenir des bornes inférieures et des garanties d'optimalité de nos réductions. Nous en déduisons ensuite des implémentations parmi les plus efficaces actuellement [S138] et qui permettent d'accélérer notamment les factorisations générales de type Choleski ($L{\cdot}D{\cdot}L^{\intercal}$). Enfin, la technique est également généralisée aux extensions d'anneaux (comme les quaternions).

4. Optimal Threshold Padlock Systems [A23], avec Jannik Dreier, Pascal Lafourcade et Léo Robert. Journal of Computer Security, volume 30:5, pages 655–688, octobre 2022.

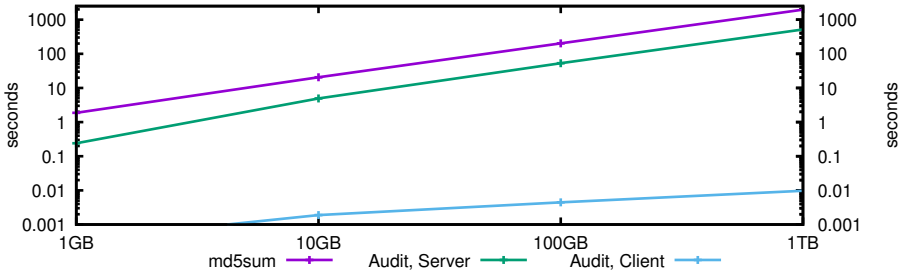
   En 1968, Liu décrivit le problème de la sécurisation de documents pour un projet secret partagé, avec un exemple nécessitant la prsénce d'au moins 6 personnes parmi 11 pour permettre un accès aux documents. Shamir a proposé la solution mathématique du partage de secret par interpolation à ce problème physique en 1979. Liu et Shamir ont affirmé que toute solution physique à ce problème devait forcément être exponentielle et impraticable sur l'exemple donné. Dans cet article, nous assouplissons certaines hypothèses implicites de cette affirmation et proposons des solutions physiques optimales de ces types de problèmes n'utilisant jamais plus de cadenas que de personnes impliquées (dans l'exemple de Liu nous n'avons par exemple besoin que de 11 cadenas). Plus généralement nous donnons des bornes inférieures plutôt logarithmiques en le nombre de participants pour des systèmes à seuil génériques. Nous donnons des solutions atteignant ces bornes pour un seuil de 2 parmi n, ou du même ordre de grandeur pour des seuils plus

importants. En dehors du monde physique, nos résultats montrent également qu'il est possible de mettre en place un partage de secret par interpolation sur des petits corps.



Un partage de secret à seuil : tous 2 parmi 5 suffisent pour obtenir le secret, avec seulement 4 cadenas (4 points d'interpolation) et chacun des 5 participants ayant 2 clefs (2 évaluations d'un polynôme de degré 3).

5. Dynamic proofs of retrievability with low server storage [A48], avec Gaspard Anthoine, Michael Hanling, Mélanie de Jonghe, Aude Maignan, Clément Pernet, et Daniel S. Roche. SECURITY 2021 : 30th USENIX Security Symposium, pages 537–554, virtual event, 11–13 Août 2021.
Les preuves de récupérabilité sont des protocoles qui permettent à un client léger de stocker de grandes quantités de données à distance (avec mises à jour) tout en s'assurant efficacement de leur intégrité (audits). La difficulté est d'avoir des protocoles rapides tant pour les lectures/écritures que pour les audits, mais un ayant surcoût de stockage raisonnable sur le serveur. Nous avons démontré qu'un compromis est inéluctable entre ces deux aspects, rapidité/stockage. Nous avons ensuite proposé le premier protocole utilisable en pratique, car avec surcoût de stockage seulement un faible pourcentage de la base de donnée, tout en conservant des temps d'audit raisonnables, autour de quelques millisecondes pour le client [S140, S136, A47].



Quelques milli-secondes suffisent à un client pour vérifier l'intégrité de tera-octets de données distantes, sans les télécharger, même en contexte malveillant.

Collaborations au sein de projets académiques et industriels

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

Start-up Notare SigNum

Issu de nos développements théoriques sur les architectures de sécurité locales [A55, A26], le projet NOTARE/ASTEROIDE ambitionne de développer un logiciel de signature électronique doté d'une force probante opposable aux tiers, assurant ainsi une confiance totale au-delà des normes actuelles définies par le règlement eIDAS. Nous avons comme objectif de fournir une technologie transférable sous licence open source, liée avec un débouché industriel à court terme, par la création d'une DEEPTECH qui générera des retombées socio-économiques.

— Déclaration d'invention **Notari signum**, 22 novembre 2023.

— Levée de fonds via la **SATT Clermont-Auvergne Inovation**, 152 k€, avril 2024.

— Levée de fonds via la bourse **BPI French Tech Lab**, 120 k€, juillet 2024.

— Levée de fonds via l'**Institut Carnot LSI (Logiciels & Systèmes Intelligents)**, 77 k€, novembre 2024.

— Levée de fonds via la bourse **BPI French Tech Emergence**, 90 k€, juin 2025.

Sécurité, cryptologie, codes, arithmétique.

14. 2024-2025 Partenariat Hubert Curien Ulysses – **CiRMCaSfCA** [P108] : complexity in rank-metric codes and semifields for cryptographic applications.
13. 2023-2028 projet PEPR Cybersécurité - **Cryptanalyse** [P111].
12. 2023-2026 Projet IRGA – **PoWaPOoS** [P122] : Protection of Whistleblowers and Private Operations on Sets.
11. 2021-2025 Projet ANR – **Sangria** [P112] : Secure distributed computation.
10. 2018 Consensys [P115].
9. 2017-2026 Cross Disciplinary Program Grenoble Alpes – **Cyber@Alps** [P123] : Grenoble Alpes Cybersecurity Institute.
8. 2017 Dolphin [P116]
7. 2014-2018 Projet Investissement d'Avenir – **ARAMIS** [P119] : Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles.
6. 2016 @GP [P117].
5. 2015 Tiempo [P118].
4. 2011-2012 Projet Grenoble universités – **MPLLC** [P124] : Multi-Precision Library for Lattices and Cryptography (co-responsable).
3. 2009-2011 Projet Ministère de l'industrie – **SHIVA** [P120] : Secured Hardware Immune Versatile Architecture.
2. 2008-2009 Projet Grenoble universités – **PALOALTO** [P127] : Plateforme d'Attaques LOgicielles par ALgorithmes et Techniques Optimisés pour architectures Multi-Coeurs Parallèles (co-responsable).
1. 2006-2009 Projet ANR – **BGPR-SAFESCALE** [P114] : certification et tolérance aux fautes sur grille de calcul.

Conception et modélisation logicielles, algorithmique parallèle.

5. 2015-2020 Projet Européen – **OPENDREAMKIT** [P109] : Open Digital Research Environment Toolkit for the Advancement of Mathematics.
4. 2010-2012 Projet CNRS-PEPS – //**INBOX** [P125] : Outils logiciels pour le calcul algébrique haute performance.
3. 2005-2008 Projet Région dans le Cluster ISLE [P128] : **CALCUL HAUTES PERFORMANCES ET INFORMATIQUE DISTRIBUÉE**.
2. 2005-2007 Projet IMAG – **AHA** [P130] : Algorithmes Hybrides Adaptatifs.
1. 2003-2004 Projet IMAG – **INCA** [P131] : Interfaces pour le calcul formel (co-responsable).

Algèbre linéaire exacte.

3. 2012-2015 Projet ANR – **HPAC** [P113] : Calcul Algébrique Haute-Performance (coordinateur).
2. 2012-2014 équipe associée INRIA-NSF – **QOLAPS** [P106] : Quantfier elimination, Optimization, Linear Algebra and Polynomial Systems.
1. Depuis 1998 Projet international CNRS-NSF-NSERC LINBOX [S141] : algèbre linéaire creuse.

Algorithmes symboliques-numériques.

5. 2008-2009 Projet Grenoble universités – **CARESSE** [P126] : Contrôle et Analyse de Réseaux de Systèmes Dynamiques Évolutifs.
4. 2005-2008 Projet Région – **CALCUL CELLULAIRE** [P129].
3. 2002-2006 Laboratoire Franco-Chinois [P107].
2. 2003-2004 Projet européen – **COMPUTATION AND CONTROL** [P110].
1. 2002-2003 Projet CNRS – **ANALYSE DES SYSTÈMES HYBRIDES** [P132] (coordinateur).

RAYONNEMENT

Activité éditoriales et de conseil scientifique

Éditeur associé

- *ACM Communications in Computer Algebra*, depuis 2006.
- *Maple Transactions*, depuis 2021.

Conseil scientifique national et international

- RCN - *Research Council of Norway*, 2024.
- HUJI - *The Hebrew University of Jerusalem*, 2024.
- AUB - *American University of Beirut*, 2024, 2020.
- CNRS - Commission régionale d'interclassement BAP E, 2024, 2022, 2021.
- ANR - Agence nationale de la recherche, 2023, 2022, 2019, 2018, 2017, 2016, 2015.
- FWF - *Fonds zur Förderung der wissenschaftlichen Forschung* (Austrian Science Fund), 2020, 2017, 2016, 2012.
- ANRT - Association Nationale de la Recherche et de la Technologie, 2019.
- Région Nouvelle-Aquitaine, 2019.
- NSERC - *Natural Sciences and Engineering Research Council of Canada*, 2018, 2016, 2013.
- Cyber@Alps - Grenoble Alpes Cybersecurity Institute (membre du comité scientifique), depuis 2018.
- Inria, 2016.
- 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.
- AERES - Agence d'évaluation de la recherche et de l'enseignement supérieur, (évaluation des laboratoires LAGIS, LIFL et de leur fusion, le CRISTAL), 2013.
- SCCyPhy - équipe-action UGA, Security and Cryptology for CyberPhysical system (membre du comité scientifique), 2013-2017.
- *Grantová agentura České republiky* (Agence Tchèque de subventions), 2011.
- JNCF - Journées nationales de Calcul Formel, membre du comité scientifique, 2010-2020.
- 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, 2013-2017.
- International Linear Algebra Society (ILAS) depuis 2013.
- Association for Computing Machinery (ACM) depuis 2000.

Comités de programmes et comités de lecture internationaux

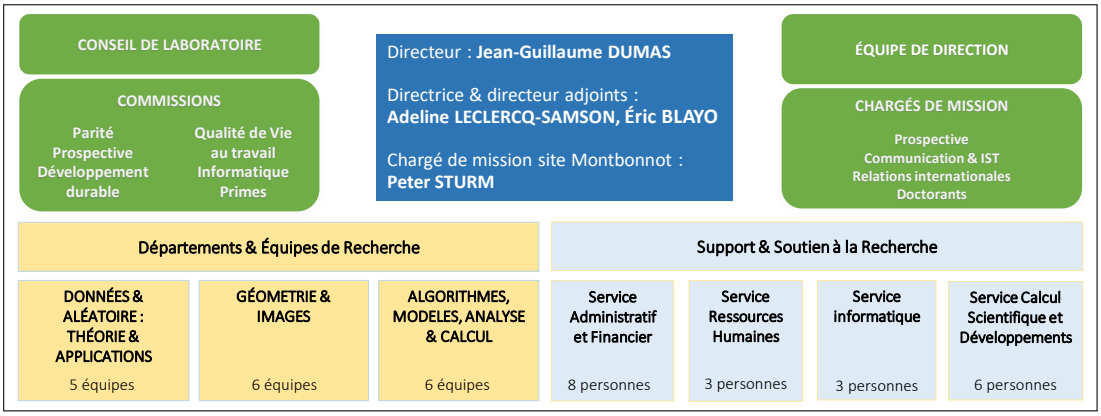
— Comités de programmes : *ISSAC 2016, 2013, 2010-2009* ; *SECURWARE 2021* ; *PASCO 2017, 2015 (chair), 2010, 2007* ; *GreHack 2017-2016* ; *Maple conf. 2022-2021* ; *LCASNC 2015 (chair)* ; *ICMC 2013* ; *PARCA 2010* ; *TC 2006* ; *OSAGC 2005*.

— Comités de lecture : *Mathematics of Computation* (2024) ; *Journal of Symbolic Computation* (2016-2015, 2013, 2008, 2006, 2003-2002, 2000) ; *ACM Transactions on Mathematical Software* (2018, 2016, 2010-2009) ; *Mathematical Reviews* (2021-2019, 2017-2016) ; *Computer Networks* (2021) ; *Journal of Computational and Applied Mathematics* (2024, 2002) ; *Information Processing Letters* (2020) ; *Designs, Codes and Cryptography* (2020) ; *Applicable Algebra in Engineering, Communication and Computing* (2020, 2010) ; *Intellectica* (2020) ; *New Generation Computing* (2024, 2021-2020) ; *Computers & Security* (2019) ; *Ad Hoc Networks* (2019) ; *Theory of Computing Systems* (2018) ; *Journal of Functional Programming* (2018) ; *IEEE Trans. on Computers* (2017) ; *Proyecciones journal of mathematics* (2017) ; *Discrete Applied Mathematics* (2012, 2010) ; *Engineering Science and Technology, an International Journal* (2016) ; *Special Matrices* (2014) ; *Annals of telecommunications* (2013) ; *The Computer Journal* (2013, 2011) ; *Mathematics and Computers in Simulation* (2012) ; *Parallel Computing* (2011) ; *Mathematical Structures in Computer Science* (2010) ; *ACM Communications in Computer Algebra* (2013, 2011-2010, 2008-2006) ; *Missouri Journal of Mathematical Sciences* (2009) ; *Information Sciences* (2008) ; *Journal of Complexity* (2004) ; *Theoretical Computer Science Algorithms* (2003).

— Rapporteur pour les conférences internationales : *ISSAC 2025-2024,2022,2020-2018, 2016, 2013-2012, 2010-2007, 2005-2002* ; *CIAC 2025* ; *MFCS 2022* ; *PASCO 2017, 2015, 2010, 2007* ; *LCASNC 2015* ; *CASC 2013, 2003* ; *ASCM 2012* ; *ICMS 2010* ; *PARCA 2010* ; *IEEE ARITH 2007* ; *SNC 2007* ; *SYNACS 2006* ; *CALCULEMUS 2006* ; *Transgressive Computing 2006* ; *WWCA 2006* ; *IEEE HPCS 2005* ; *STACS 2002* ; *IPDPS 2001*.

Direction du Laboratoire Jean Kuntzmann

Depuis le 1er juillet 2020, je suis directeur du Laboratoire Jean Kuntzmann (UMR CNRS/UGA/G-INP 5224). Suite à la mutation de mon prédécesseur, Stéphane Labbé, j'ai en effet pris la direction un peu avant la fin de son mandat (initialement prévue au 31 décembre 2020).
Le laboratoire est situé sur deux sites, campus (bâtiment IMAG) et Monbonnot (bâtiment Inria). Nous sommes organisés en 17 équipes de recherche, regroupées en 3 départements, et 4 services de support et soutien à la recherche (Administratif et financier, Ressources humaines, Informatique systèmes et réseaux, Calcul scientifique). Au total cela représente plus de 300 personnes, avec environ 140 permanents (dont une vingtaine de personnels d'accompagnement), une centaine de doctorants, post-doctorants et chercheurs sur contrats, et une soixantanie de stagiaires. Hors masse salariale, le budget annuel du LJK est d'environ 3,5 millions d'euros dont 90% de ressources contractuelles.
Le début de mon mandat a bien sûr été marqué par la crise sanitaire qui venait de débuter et par les précautions particulières afférentes (consignes, signalements, masques, tests, capteurs CO_2, etc.), ainsi que par la gestion des locaux (principalement sur le site campus, le second étant du ressort d'Inria), des justificatifs, des recensements, des permanences, et par le développement du télétravail.
Au niveau de l'organigramme, nous travaillons au quotidien en équipe de direction comportant une directrice adjointe et un directeur adjoint, un chargé de mission pour le site de Monbonnot et de quatre responsables de services. Puis plus largement en un conseil de laboratoire élu, une assemblée des responsables d'équipes bimestrielle et une assemblée générale annuelle, comme illustré sur le graphique suivant.



Afin de donner le plus de transparence possible à notre travail de pilotage scientifique et stratégique, nous avons mis en place plusieurs commissions, pour la plupart dépendantes du conseil de laboratoire, afin de traiter des sujets de primes, de promotions, de prospective (emplois), de développement

durable, de parité, de qualité de vie au travail, de prévention des risques y compris psycho-sociaux, d'élections, de doctorants et nouveaux arrivants ou encore d'animation scientifique (mois de stages, colloques, invitations, etc.). Plus généralement lorsqu'un classement ou un arbitrage est nécessaire, nous avons la plupart du temps une discussion collective, en comité de direction, en conseil ou en commission, en associant éventuellement également une participation syndicale.
En tant que DU, plusieurs responsabilités sont bien sûr fondamentales, de la gestion des infrastructures (bâtiment IMAG notamment, avec la direction du patrimoine de l'UGA et du partenaire privé propriétaire), des urgences (plan de sobriété, alarmes, DUERP, plan de reprise et continuation, responsabilités sanitaires), au plan de formation, et à la définition du budget.
Ceci implique des relations avec les différentes tutelles et des stratégies locales et nationales (CNRS DR11, Insmi, Ins2i, UGA, Grenoble-INP, Inria), permettant un dialogue de gestion et une politique salariale adossés aux campagnes emplois C, E-C et BIATSS. Cela s'accompagne de bonnes relations avec les unités de formation (UFR IM2AG, Ensimag, Économie, SHS, etc.), avec les laboratoires (du pôle MSTIC à Grenoble, de mathématiques au niveau régional ou national) et de partenaires privilégiés à l'international ou encore avec les infrastructures partagées (agence AMIES, data center IMAG, UAR Gricad, etc.).
Au niveau des services, nous avons plusieurs spécificités au sein du LJK : un service calcul propose un accompagnement et du soutien aux projets de recherche du laboratoire, et nous avons créé également un service dédié aux ressources humaines avec des champs d'action larges, un rôle de conseil et d'accompagnement à tous les niveaux (contrats, relations interpersonnelles, entretiens individuels, cas sensibles, suivi, prévention et médiation quelquefois, santé et social lourd parfois, jusqu'à une occurrence de contexte policier et judiciaire).
Enfin il me semble que la mission majeure consiste à soutenir l'ensemble des personnels de l'unité, que ce soit dans leurs projets, de recherche, de mobilité, d'invitations ou plus prosaïquement pour les primes, les avancements ou les entretiens annuels.

Direction adjointe du Laboratoire Jean Kuntzmann

Du 1er janvier 2014 au 31 décembre 2016, j'ai été directeur adjoint du Laboratoire Jean Kuntzmann (UMR 5224), 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.
Du 1er janvier 2020 au 30 juin 2020, j'ai également été directeur adjoint du Laboratoire Jean Kuntzmann en charge des aspects de recherche.

Responsabilité d'équipe de recherche

Durant le quadriennal 2006-2009, et entre 2017 et 2020, j'ai été responsable de l'équipe CASYS (Calculs Algébriques et Systèmes Dynamiques) puis nous avons créé l'équipe CAS^{3}C^3 (Calcul Algébrique et Symbolique, Sécurité, Systèmes Complexes, Codes et Cryptologie) au sein du département Algorithmes, Modèles, Analyse et Calcul du LJK. L'équipe regroupe une dizaine de chercheurs permanents et une dizaine de doctorants, post-doctorants ou ingénieurs.

Commission de spécialistes, conseil d'UFR, conseil de laboratoire

- 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.
- Titulaire élu du conseil de laboratoire du LJK, 2017-2019.
- Plusieurs comités de sélection, U. Grenoble Alpes, U. Clermont Auvergne, U. Lille, Sorbonne U., U. Limoges, ...

Responsabilité des moyens informatiques

De 2002 à 2007, puis de 2011 à 2014, j'ai été responsable des moyens informatiques de l'équipe MOSAIC, puis CASYS du LJK. En son sein, j'ai géré un parc d'une vingtaine de stations de travail PC (Linux Debian/Mandrake/Ubuntu, des Windows XP/Vista/Win7, des Apple powerbook), des DEC alpha et des serveurs SUN solaris.

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, puis de la RIPEC C3 2023-2026.
- Accessit au concours général de mathématiques 1992.

Organisation de conférences

RTCAm3 2023, LCASNC 2015, ILAS2013, ACM ISSAC2012, SIAM AAG2011, ACM ISSAC2011, JNCF2010, ACM PASCO2010, DubLinBox2010, ACM ISSAC2009, JNCF2008, SIAM PPSC2006, ACM ISSAC2006, Transgressive Computing 2006, CalSym2005, EJCACF2004, JNCF2003.

Communications, invitations et séjours de recherche internationaux

44. 7 – 14 décembre 2024 : Collaboration avec John Sheekey et Stefano Lia, University College Dublin, Irlande.

43. 20 – 24 juin 2022 : *Dynamic proofs of retrievability & verified evaluation of secret dotproducts & polynomials*. The 24th conference of the International Linear Algebra Society (ILAS 2022), Galway, Irlande.

42. 9 février 2022 : *Low-storage dynamic proofs of retrievability*. Brave research, San Francisco, USA.

41. 3 – 7 août 2021 : *The forking effect* (avec S. Jimenez Garces, M. Mourey et F. Şoiman). World Finance Conference (WFC21), Agder, Norvège.

40. 17 – 21 mai 2021 : *LU Factorization with Errors by Means of Reduction to Fast Matrix Multiplication* (avec J. v. d. Heoven, C. Pernet et D. Roche). SIAM Conference on Applied Linear Algebra (LA21), New Orleans, USA.

39. 17 – 21 mai 2021 : *On Fast Multiplication of a Matrix by its Transpose Or Conjugate Transpose* (avec C. Pernet et A. Sedoglavic). SIAM Conference on Applied Linear Algebra (LA21), New Orleans, USA.

38. 11 – 15 novembre 2019 : *Proofs of Retrievability with Low Server Storage* (avec Mike Hanling, Gaspard Anthoine, Aude Maignan, Clément Pernet, et Daniel S. Roche). The 26th ACM Conference on Computer and Communications Security (CCS'19), Londres, UK.

37. 17 – 21 septembre 2018 : *Proof-of-work certificates that can be efficiently computed in the cloud*, The 20th International Workshop on Computer Algebra in Scientific Computing (CASC'18), Lille, France.

36. 15 – 25 juillet 2016 : *Efficient bootstrapping for matrix-vector public verification*. Milestones in Computer Algebra (MICA 2016), Waterloo, Canada.

35. Automne 2015 : Invitation au Fields Institute, Toronto, Canada, 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

62. *Fast in-place accumulation* (avec Bruno Grenet). Séminaire CAS^{3}C^3, 10 octobre 2024, Grenoble, France.

61. *libVESPo: a C++ library for the Verified Evaluation of Secret Polynomials*. Mathematical Software and High Performance Algebraic Computing (RTCA), Lyon, France, 26–20 juin 2023.

60. *The forking effect* (avec Sonia Jimenez Garces, Mathis Mourey et Florentina Şoiman). The 39th International Conference of the French Finance Association (AFFI), Bordeaux, France, 5–7 juin 2023.

59. *Cryptomonnaies et NFT : mythes ou réalités ?* CCI îles de guadeloupe, France, 10 Octobre 2022.

58. *Preuves de récupérabilité dynamique & évaluation vérifiée de polynômes secrets* (avec Aude Maignan et Clément Pernet). Séminaire ECO, Montpellier, France, 1er juin 2022.

57. *The returns of (I)DeFiX* (avec Sonia Jimenez Garces et Florentina Şoiman). The 38th International Conference of the French Finance Association (AFFI), Saint-Malo, France, 23–25 mai 2022.

56. *Fast multiplication of a matrix by its transpose* (avec Clément Pernet et Alexandre Sedoglavic). Journées nationales de calcul formel, 2-6 mars 2020, Luminy, France.

55. *La sécurité des blockchains*. Parcours Innovateur, Ensimag, Grenoble, France, 14 février 2020.

54. *Produit d'une matrice par son adjointe* (avec Clément Pernet et Alexandre Sedoglavic). Séminaire CAS^{3}C^3, 16 janvier 2020, Grenoble, France.

53. *Calcul formel et symbolique* (avec Françoise Jung et Clément Pernet). Journée histoire du calcul, Grenoble, France, 28 novembre 2019.

52. *Sécurité des blockchains, panorama des attaques et aspects financiers*. Cybersecurity Institute, Grenoble, France, 2 avril 2019.

51. *Les blockchains, des systèmes distribués*. Parcours Innovateur, Ensimag, Grenoble, France, 15 mars 2019.

50. *C++ haute-performance*. Formation Dolphin, Grenoble, France, 29-30 novembre 2017.

49. *Architectures de sécurité*. Formation @GP, Montélier, 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://membres-ljk.imag.fr/Jean-Guillaume.Dumas/publications.html

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

[A1] Jean-Guillaume Dumas et Bruno Grenet. – In-place accumulation of fast multiplication formulae. Dans : **ISSAC'2024** [155 - Chen (2024)], pages 16–25.

[A2] Jean-Guillaume Dumas et Bruno Grenet. – In-place fast polynomial modular remainder. Dans : **ISSAC'2024** [155 - Chen (2024)], pages 26–35.

[A3] Jean-Guillaume Dumas, Clément Pernet et Alexandre Sedoglavic. – Strassen's algorithm is not optimally accurate. Dans : **ISSAC'2024** [155 - Chen (2024)], pages 254–263.

[A4] Jean-Guillaume Dumas, Clément Pernet et Alexandre Sedoglavic. – On fast multiplication of a matrix by its transpose. Dans : **ISSAC'2020** [162 - Leykin (2020)], pages 162–169.

[A5] Jean-Guillaume Dumas, Joris van der Hoeven, Clément Pernet et Daniel S. Roche. – LU factorization with errors. Dans : **ISSAC'2019** [161 - Kauers (2019)], pages 131–138.

[A6] Jean-Guillaume Dumas et Clément Pernet. – Symmetric indefinite elimination revealing the rank profile matrix. Dans : **ISSAC'2018** [154 - Arreche (2018)], pages 151–158.

[A7] 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** [167 - Safey El Din (2017)], pages 125–132.

[A8] Jean-Guillaume Dumas, David Lucas et Clément Pernet. – Certificates for triangular equivalence and rank profiles. Dans : **ISSAC'2017** [167 - Safey El Din (2017)], pages 133–140.

[A9] 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** [156 - Gao (2016)], pages 199–206.

[A10] Jean-Guillaume Dumas, Clément Pernet et Ziad Sultan. – Computing the rank profile matrix. Dans : **ISSAC'2015** [169 - Yokoyama (2015)], pages 149–156. **Distinguished paper award**.

[A11] Jean-Guillaume Dumas et Erich Kaltofen. – Essentially optimal interactive certificates in linear algebra. Dans : **ISSAC'2014** [166 - Nabeshima (2014)], pages 146–153.

[A12] Jean-Guillaume Dumas, Clément Pernet et Ziad Sultan. – Simultaneous computation of the row and column rank profiles. Dans : **ISSAC'2013** [160 - Kauers (2013)], pages 181–188.

[A13] Brice Boyer, Jean-Guillaume Dumas, Clément Pernet et Wei Zhou. – Memory efficient scheduling of Strassen-Winograd's matrix multiplication algorithm. Dans : **ISSAC'2009** [163 - May (2009)], pages 135–143.

[A14] Jean-Guillaume Dumas, Clément Pernet et B. David Saunders. – On finding multiplicities of characteristic polynomial factors of black-box matrices. Dans : **ISSAC'2009** [163 - May (2009)], pages 55–62.

[A15] Jean-Guillaume Dumas. – Q-adic transform revisited. Dans : **ISSAC'2008** [158 - Jeffrey (2008)], pages 63–69.

[A16] Jean-Guillaume Dumas, Clément Pernet et Zhendong Wan. – Efficient computation of the characteristic polynomial. Dans : **ISSAC'2005** [159 - Kauers (2005)], pages 140–147.

[A17] Jean-Guillaume Dumas et Aude Rondepierre. – Algorithms for symbolic/numeric control of affine dynamical systems. Dans : **ISSAC'2005** [159 - Kauers (2005)], pages 277–284.

[A18] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – FFPACK: Finite field linear algebra package. Dans : **ISSAC'2004** [157 - Gutierrez (2004)], pages 119–126.

[A19] Jean-Guillaume Dumas, Thierry Gautier et Clément Pernet. – Finite field linear algebra subroutines. Dans : **ISSAC'2002** [164 - Mora (2002)], pages 63–74.

[A20] 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** [168 - Traverso (2000)], pages 95–105.

[A21] Jean-Guillaume Dumas, Sonia Jimenez-Garces et Florentina Şoiman. – What drives DeFi market returns? **Journal of International Financial Markets, Institutions & Money**, volume 85, juin 2023, page 101786.

[A22] Jean-Guillaume Dumas, Clément Pernet et Alexandre Sedoglavic. – Some fast algorithms multiplying a matrix by its adjoint. **Journal of Symbolic Computation**, volume 115, mars 2023, pages 285–315.

[A23] Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade et Léo Robert. – Optimal Threshold Padlock Systems. **Journal of Computer Security**, volume 30, n° 5, octobre 2022, pages 655–688.

[A24] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. – A faster cryptographer's conspiracy Santa. **Theoretical Computer Science**, volume 839, 2 novembre 2020, pages 122–134.

[A25] Jean-Guillaume Dumas, Erich L. Kaltofen, David Lucas et Clément Pernet. – Elimination-based certificates for triangular equivalence and rank profiles. **Journal of Symbolic Computation**, volume 98, mai–juin 2020, pages 246 – 269.

[A26] Jean-Guillaume Dumas, Pascal Lafourcade, Francis Melemedjian, Jean-Baptiste Orfila et Pascal Thoniel. – LocalPKI: An interoperable and IoT friendly PKI. **E-Business and Telecommunications**, volume 990, 2019, pages 224–252.

[A27] 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.

[A28] 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.

[A29] 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.

[A30] 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.

[A31] 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.

[A32] 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.

[A33] 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.

[A34] 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.

[A35] 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.

[A36] 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.

[A37] 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.

[A38] 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.

[A39] 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.

[A40] 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.

[A41] 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.

[A42] 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.

[A43] 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

[A44] Jean-Guillaume Dumas. – Les rayons des permutations spirales. **Mathématiques et Sciences Humaines**, volume 192, n° 4, 2010, pages 5 – 27.

[A45] Jean-Guillaume Dumas. – Caractérisation des quenines et leur représentation spirale. **Mathématiques et Sciences Humaines**, volume 184, n° 4, 2008, pages 9 – 23.

Autres conférences internationales avec comité de lecture et actes publiés

---

[A46] Jean-Guillaume Dumas, Alexis Galan, Bruno Grenet, Aude Maignan et Daniel S. Roche. – Communication optimal unbalanced private set union. Dans : **23rd International Conference on Applied Cryptography and Network Security (ACNS 2025)**, Marc Fischlin et Veelasha Moonsamy éd., 23–26 juillet 2025, pages –30. – Munich, Germany.

[A47] Jean-Guillaume Dumas, Aude Maignan, Clément Pernet et Daniel S. Roche. – VESPo: Verified evaluation of secret polynomials: with application to low-storage dynamic proofs of retrievability. Dans : **23rd Privacy Enhancing Technologies Symposium (PETS 2023)**, 10–15 juillet 2023, pages 354–374. – Lausanne, Switzerland.

[A48] Gaspard Anthoine, Jean-Guillaume Dumas, Michael Hanling, Mélanie de Jonghe, Aude Maignan, Clément Pernet et Daniel S. Roche. – Dynamic proofs of retrievability with low server storage. Dans : **30th USENIX Security Symposium, August 11-13**, août 2021. Pages 537–554. – USENIX Association.

[A49] Jean-Guillaume Dumas, Sonia Jimenez-Garces et Florentina Şoiman. – Blockchain technology and cryptomarket: vulnerabilities and risk assessment. Dans : **12th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC Conference 2021)**, Nagib Callaos et Hsing-Wei Chu éd., 9–12 mars 2021, pages 30–37. – Orlando, Florida, United States.

[A50] Jean-Guillaume Dumas, Pascal Lafourcade, Julio López Fenner, David Lucas, Jean-Baptiste Orfila, Clément Pernet et Maxime Puys. – Secure multi-party matrix multiplication based on Strassen-Winograd algorithm. Dans : **The 14th International Workshop on Security (IWSEC 2019), A: Cryptography Track**, Nuttapong Attrapadung et Takeshi Yagi éd., 28–30 août 2019. – *Lecture Notes in Computer Science, Advances in Information and Computer Security*, volume 11689, pages 67–88. – Tokyo, Japan.

[A51] Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki et Hideaki Sone. – Interactive physical zero-knowledge proof for norinori. Dans : **The 25th International Computing and Combinatorics Conference (COCOON 2019)**, Dingzhu Du, Zhenhua Duan et Cong Tian éd., 4–7 juillet 2019. – *Lecture Notes in Computer Science*, volume 11653, pages 166–177. – Xian, China.

[A52] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. – A cryptographer's conspiracy Santa. Dans : **9th International conference on Fun with algorithms (FUN 2018)**, Hiro Ito, Stefano Leonardi, Linda Pagli et Giuseppe Prencipe éd., 13–15 juin 2018. – *Leibniz International Proceedings in Informatics (LIPIcs)*, volume 100, pages 13:1–13:13. – Maddalena, Italy.

[A53] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa et Hideaki Sone. – Physical zero-knowledge proof for Makaro. Dans : **20th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2018)**, Taisuke Izumi et Petr Kuznetsov éd., 4–7 novembre 2018. – *Lecture Notes in Computer Science*, volume 11201, pages 111–125. – Tokyo, Japan.

[A54] 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 (WCICSS 2017)**, 11–14 décembre 2017, pages 22–29. – Cambridge, UK.

[A55] 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)**, Pierangela Samarati éd., 24–26 juillet 2017. – *ICETE 2017*, pages 187–199. – Madrid, Spain.

[A56] Jean-Guillaume Dumas et Vincent Zucca. – Prover efficient public verification of dense or sparse/structured matrix-vector multiplication. Dans : **22nd Australasian Conference on Information Security and Privacy (ACISP 2017)**, Josef Pieprzyk et Suriadi Suriadi éd., 3–7 juillet 2017. – *Lecture Notes in Computer Science*, volume 10343, pages 115–134. – Auckland, New Zealand.

[A57] Alexis Breust, Christophe Chabot, 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. – *Lecture Notes in Computer Science*, volume 9725, pages 223–231. – Berlin, Germany.

[A58] Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas et 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. – Maddalena, Italy.

[A59] 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)**, Pierangela Samarati éd., 26–28 juillet 2016. – *ICETE 2016*, volume 4, pages 61–72. – Lisbon, Portugal. **Best paper award**.

[A60] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici, Damien Pous et Jean-Claude Reynaud. – Relative Hilbert-Post completeness for exceptions. Dans : **Sixth International Conference on Mathematical Aspects of Computer and Information Sciences (MACIS 2015)**, S. Ilias Kotsireas, M. Siegfried Rump et K. Chee Yap éd., 11–13 novembre 2015. – *Lecture Notes in Computer Science*, pages 596–610. – Berlin, Germany.

[A61] 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 : **Proceedings of the 2014 International Congress of Mathematical Software (ICMS'2014)**, Hoon Hong et Chee K. Yap éd., 5–9 août 2014. – *Lecture Notes in Computer Science*, volume 8592, pages 654–662. – Seoul, Korea.

[A62] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici et Jean-Claude Reynaud. – Certified proofs in programs involving exceptions. Dans : **Proceedings of the 2014 Conference on Intelligent Computer Mathematics (CICM-WIP'2014)**, 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. – Coimbra, Portugal.

[A63] Jean-Guillaume Dumas, Thierry Gautier, Clément Pernet et Ziad Sultan. – Parallel computation of echelon forms. Dans : **Proceedings of the 20th international conference on parallel processing (Euro-Par'2014)**, Fernando Silva, Inês Dutra et Vítor Santos Costa éd., 25–29 août 2014. – *Lecture Notes in Computer Science*, volume 8632, pages 499–510. – Porto, Portugal.

[A64] Jannik Dreier, Jean-Guillaume Dumas et Pascal Lafourcade. – Attacking privacy in a fully private auction protocol. Dans : **Proceedings of the sixth International Conference on Cryptology in Africa (AfricaCrypt'2013)**, Amr Youssef et Abderrahmane Nitaj éd., 22–24 juin 2013. – *Lecture Notes in Computer Science*, volume 7918, pages 88–106. – Cairo, Egypt.

[A65] 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.

[A66] Jean-Guillaume Dumas et Hicham Hossayni. – Matrix powers algorithm for trust evaluation in PKI architectures. Dans : **Proceedings of the eigth International Workshop on Security and Trust Management (STM'2012, co-ESORICS)**, Audun Jøsang, Pierangela Samarati et Marinella Petrocchi éd., 13–14 septembre 2012. – *Lecture Notes in Computer Science*, volume 7783, pages 129–144. – Pisa, Italy.

[A67] Brice Boyer, Jean-Guillaume Dumas et Pascal Giorgi. – Exact sparse matrix-vector multiplication on GPU's and multicore architectures. Dans : **PASCO'10** [165 - Moreno-Maza et Roch (2010)], pages 80–88.

[A68] Jean-Guillaume Dumas, Thierry Gautier et Jean-Louis Roch. – Generic design of chinese remaindering schemes. Dans : **PASCO'10** [165 - Moreno-Maza et Roch (2010)], pages 26–34.

[A69] Alexandre Berzati, Cécile Canovas, Jean-Guillaume Dumas et Louis Goubin. – Fault attacks on RSA public keys: Left-to-right implementations are also vulnerable. Dans : **Proceedings of the RSA Conference, Cryptographers' Track (CTRSA'2009)**, Marc Fischlin éd., 20–24 avril 2009. – *Lecture Notes in Computer Science*, volume 5473, pages 414–428. – San Francisco, USA.

[A70] Jean-Guillaume Dumas, Laurent Fousse et Bruno Salvy. – Compressed modular matrix multiplication. Dans : **Milestones in Computer Algebra (MICA 2008)**, Mark Giesbrecht et Stephen Watt éd., 1–3 mai 2008, pages 133–140. – Tobago.

[A71] 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 : **Proceedings of the 3rd ACM International Workshop on Parallel Symbolic Computation (PASCO'07)**, Marc Moreno-Maza et Stephen Watt éd., 26–27 juillet 2007. Pages 43–52. – Waterloo University, Ontario, Canada.

[A72] 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** [L105], pages 131–148.

[A73] Jean-Guillaume Dumas et Anna Urbańska. – An introspective algorithm for the determinant. Dans : **TC'2006** [L105], pages 185–202.

[A74] Jean-Guillaume Dumas. – Efficient dot product over finite fields. Dans : **Proceedings of the seventh International Workshop on Computer Algebra in Scientific Computing (CASC'2004)**, Victor G. Ganzha, Ernst W. Mayr et Evgenii V. Vorozhtsov éd., 12–19 juillet 2004. Pages 139–154. – Saint Petersburg, Russia.

[A75] Jean-Guillaume Dumas et Aude Rondepierre. – Modeling the electrical activity of a neuron by a continuous and piecewise affine hybrid system. Dans : **Proceedings of the 2003 Hybrid Systems: Computation and Control (HSCC'2003)**, Oded Maler et Amir Pnueli éd., 3–5 avril 2003. – *Lecture Notes in Computer Science*, volume 2623, pages 156–171. – Prague, The Czech Republic.

[A76] 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 : **Proceedings of the 2002 International Congress of Mathematical Software (ICMS'2002)**, Arjeh M. Cohen, Xiao-Shan Gao et Nobuki Takayama éd., 17–19 août 2002. Pages 40–50. – Beijing, China.

[A77] Jean-Guillaume Dumas et Gilles Villard. – Computing the rank of sparse matrices over finite fields. Dans : **Proceedings of the fifth International Workshop on Computer Algebra in Scientific Computing (CASC'2002)**, Victor G. Ganzha, Ernst W. Mayr et Evgenii V. Vorozhtsov éd., 22–27 septembre 2002. Pages 47–62. – Yalta, Ukraine.

[A78] Jean-Guillaume Dumas et Jean-Louis Roch. – A fast parallel block algorithm for exact triangularization of rectangular matrices. Dans : **Proceedings of the Thirteenth ACM Symposium on Parallel Algorithms and Architectures (SPAA'01)**, Pierre Fraigniaud éd., 4–6 juillet 2001, pages 324–325. – Kreta, Greece.

Conférences nationales avec comité de lecture et actes publiés

[B79] Jean-Guillaume Dumas, Dominique Duval, Burak Ekici et Damien Pous. – Formal verification in Coq of program properties involving the global state effect. Dans : **25e Journées Francophones des Langages Applicatifs (JFLA 2014)**, Christine Tasson éd., 8–11 janvier 2014, pages 1–15. – Fréjus, France.

[B80] Jean-Guillaume Dumas et Dominique Duval. – Towards a diagrammatic modeling of the LinBox C++ linear algebra library. Dans : **Langages et Modèles à Objets (LMO'2006)**, Roger Rousseau, Christelle Urtado et Sylvain Vauttier éd., 22–24 mars 2006. Pages 117–132. – Nîmes, France.

[B81] Jean-Guillaume Dumas. – Calcul parallèle du polynôme minimal entier en Athapascan-1 et LinBox. Dans : **Actes des douzièmes rencontres francophones du parallélisme (RENPAR12)**, Herv'e Guyennet éd., 19-22 juin 2000. – *TSI, Technique et science informatiques*, volume 20, pages 119–124. – Besançon, France.

Conférences internationales invitées avec actes publiés

[B82] Jean-Guillaume Dumas. – Proof-of-work certificates that can be efficiently computed in the cloud. Dans : **Proceedings of the 20th International Workshop on Computer Algebra in Scientific Computing (CASC'2018)**, Vladimir P. Gerdt, Wolfram Koepf, Werner M. Seiler et Evgenii V. Vorozhtsov éd., 17–21 septembre 2018. – *Lecture Notes in Computer Science*, volume 11077, pages 1–17. – Lille, France.

[B83] Jean-Guillaume Dumas, Thierry Gautier, Clément Pernet et B. David Saunders. – LinBox founding scope allocation, parallel building blocks, and separate compilation. Dans : **Proceedings of the 2010 International Congress of Mathematical Software (ICMS'2010)**, Komei Fukuda, Joris vander Hoeven, Michael Joswig et Nobuki Takayama éd., 13–17 septembre 2010. – *Lecture Notes in Computer Science*, volume 6327, pages 77–83. – Kobe, Japan.

[B84] 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

[L85] Jean-Guillaume Dumas, Pascal Lafourcade, Étienne Roudeix, Ariane Tichit et Sébastien Varrette. – ***Les NFT en 40 questions : comprendre les jetons non fongibles***. – Dunod, 2022, 256 pages.

[L86] Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit et Sébastien Varrette. – ***Les blockchains en 50 questions : comprendre les enjeux de cette technologie innovante***. – Dunod, 2022, 2e édition, 320 pages.

[L87] Jean-Guillaume Dumas, Pascal Lafourcade et Patrick Redon. – ***Architectures de sécurité pour internet : protocoles, standards et déploiement***. – Dunod, juillet 2020, *InfoSup*, 432 pages.

[L88] Jean-Guillaume Dumas, Pascal Lafourcade, Ariane Tichit et Sébastien Varrette. – ***Les blockchains en 50 questions : comprendre les enjeux de cette technologie innovante***. – Dunod, 2018, 304 pages.

[L89] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Théorie des codes : compression, cryptage, correction***. – Dunod, 2018, 3^{e} édition, 415 pages.

[L90] Jean-Guillaume Dumas, Pascal Lafourcade et Patrick Redon. – ***Architectures PKI et communications sécurisées***. – Dunod, 2015, 398 pages.

[L91] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Foundations of Coding: Compression, Encryption, Error-Correction***. – Wiley, USA, février 2015, 373 pages.

[L92] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Théorie des codes : compression, cryptage, correction***. – Dunod, 2013, 2^{e} édition, 384 pages.

[L93] Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier et Sébastien Varrette. – ***Théorie des codes : compression, cryptage, correction***. – Dunod, 2007, 352 pages.

Chapitres de livres

[L94] Jean-Guillaume Dumas et Clément Pernet. – Les codes détecteurs et correcteurs d'erreurs pour la fiabilité des calculs. Dans : **Le calcul à découvert**, Mokrane Bouzeghoub, Michel Daydé et Christian Jutten éd., pages 57–59. – CNRS, janvier 2025.

[L95] Jean-Guillaume Dumas et Pascal Lafourcade. – La sécurité de bitcoin et des blockchains. Dans : **Treize défis de la cybersécurité**, Gildas Avoine et Marc-Olivier Killijian éd., pages 213–232. – CNRS, juin 2020.

[L96] 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.

[L97] 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.

[L98] 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.

[L99] 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.

[L100] 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.

[L101] 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

[L102] Jean-Guillaume Dumas et Erich Kaltofen (éditeurs). – ***Proceedings of the 5th acm international workshop on parallel symbolic computation (PASCO'15)***, 10–11 juillet 2015. – ACM Press, Bath, UK.

[L103] 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.

[L104] Jean-Guillaume Dumas (éditeur). – ***ISSAC'2006, Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, Genova, Italy***, 9–12 juillet 2006. – ACM Press, New York.

[L105] Jean-Guillaume Dumas (éditeur). – ***TC'2006, proceedings of transgressive computing 2006, Granada, España***, 24–26 avril 2006. – Universidad de Granada, Spain.

Projets Internationaux

[P106] 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.

[P107] 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

[P108] U. College Dublin et L. J. Kuntzmann. – CIRMCASFCA : ***Complexity in rank-metric codes and semifields for cryptographic applications***. – 5 k€, PHC Ulysses, 2024-2025.

[P109] 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.

[P110] L. J. Kuntzmann. – CC : ***Contrôle Hybride***. Dans : **Computation and Control**. – 4 k€, Projet Européen, 2003-2004.

Projets Nationaux (ANR, PEPR)

[P111] CNRS, INRIA, U. Bordeaux, U. Grenoble-Alpes, U. Lorraine, U. Montpellier, U. Picardie Jules Verne, U. Rennes et U. Saint-Quentin en Yvelines. – CRYPTANALYSE : ***La résistance des systèmes cryptographiques***. – 25 k€, PEPR Cybersécurité, 2023-2028.

[P112] Sorbonne Université, École normale supérieure, Telecom Paris, Université de Bordeaux, Université de Limoges, Université de Montpellier et Université Grenoble Alpes. – SANGRIA : ***Secure distributed computAtioN: cryptoGRaphy, combinatorIcs and computer Algebra***. – 416 k€, ANR, ANR-21-CE39-0006, 2021-2025.

[P113] 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.

[P114] 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

[P115] Consensys. – LINNIA : ***Homomorphic computations, verifiable computing and blockchains***. – 6 k€, Contrat industriel, 2018.

[P116] Dolphin. – HPCPP : ***Formation C++ Haute performance***. – 5 k€, Contrat industriel, 2017.

[P117] @GP. – CRYPTAAPKI : ***Formation Cryptographie asymétrique et architectures de sécurité***. – 5 k€, Contrat industriel, 2016.

[P118] Tiempo-Secure. – SIDERSA : ***Formation Attaques par perturbation sur RSA embarqué***. – 6 k€, Contrat industriel, 2015.

[P119] L. Informatique de Grenoble, Verimag, L. Jean Kuntzmann, Institut Fourier, Atos, SecLab et CEA-Leti. – ARAMIS : ***Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles***. – 820 k€, Investissements d'Avenir, 2014-2018.

[P120] L. Informatique de Grenoble, Verimag, L. Jean Kuntzmann, Institut Fourier, Communication & Systems, Netheos, iWall/Mataru, EasyiiC et CEA-Leti. – SHIVA : ***Secured Hardware Immune Versatile Architecture***. – 2.2 M€, Ministère de l'industrie, 2009-2011.

[P121] 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 Régionaux

[P122] L. J. Kuntzmann. – POWAPOOS : ***Protection of Whistleblowers and Private Operations on Sets***. – 100 k€, UGA-IRGA, 2023-2026.

[P123] CEA-Leti, CERAG, CESICE, CREG, G2Elab, GIPSA-Lab, G-SCOP, Institut Fourier, INRIA, LCIS, LIG, LISTIC, LJK, PACTE, TIMA et VERIMAG. – CYBER@ALPS : ***Grenoble Alpes Cybersecurity Institute***. – 1.45 M€, Cross Disciplinary Program Grenoble Alpes, 2018-2026.

[P124] L. J. Kuntzmann et Institut Fourier. – MPLLC : ***Multi-Precision Library for Lattices and Cryptography***. – 55 k€, UJF-Pôle MSTIC, 2011-2012.

[P125] 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.

[P126] L. J. Kuntzmann. – CARESSE : ***Contrôle et Analyse de Réseaux de Systèmes Dynamiques Évolutifs***. – 65 k€, UJF-Pôle MSTIC, 2008-2009.

[P127] 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.

[P128] 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.

[P129] L. J. Kuntzmann et L. d'InfoRmatique en Image et Systèmes d'information. – CALCEL : ***Calcul Cellulaire***. – 120 k€, Région Rhône-Alpes, 2005-2008.

[P130] L. J. Kuntzmann et L. Informatique de Grenoble. – AHA : ***Algorithmes Hybrides Adaptatifs***. – 80 k€, IMAG, 2005-2007.

[P131] L. J. Kuntzmann et L. Logiciels Systèmes Réseaux. – INCA : ***Interfaces pour le calcul formel***. – 30 k€, IMAG, 2003-2004.

[P132] L. J. Kuntzmann. – SQUASH : ***Analyse qualitative des systèmes hybrides***. – 10 k€, CNRS, 2002-2003.

Logiciels (cf. https://cas3c3.imag.fr/logiciels.html)

[S133] Jean-Guillaume Dumas, Alexis Galan, Bruno Grenet, Aude Maignan et Daniel S. Roche. – CoUPSU : Communication optimal unbalanced private set union using FHE, décembre 2024. 1 kSLOC.

[S134] Jean-Guillaume Dumas, Bruno Grenet, Clément Pernet et Alexandre Sedoglavic. – PLinOpt, a collection of C++ routines handling linear & bilinear programs, janvier 2024. 3.4 kSLOC.

[S135] Jean-Guillaume Dumas, Clément Pernet et Alexandre Sedoglavic. – Matlab accurate fast matrix multiplications via 2x2 recursion, janvier 2024. 1.6 kSLOC.

[S136] Jean-Guillaume Dumas. – libVESPo: a C++ library for the verified evaluation of secret polynomials, décembre 2022. 5 kSLOC.

[S137] Jean-Guillaume Dumas. – Paillier subgroup homomorphic encryption in RELIC, février 2022. 3 kSLOC.

[S138] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – FFLAS-FFPACK 2.5.0 Sablet: Finite field linear algebra subroutine/package. – Debian (`fflas-ffpack`), décembre 2021. 68 kSLOC.

[S139] Jean-Guillaume Dumas, Pascal Giorgi et Clément Pernet. – Givaro-4.2.0 Sablet, a C++ library for computer algebra: exact arithmetic and data structures. – Debian (`libgivaro1, libgivaro-dev`), décembre 2021. 47 kSLOC.

[S140] Jean-Guillaume Dumas, Michael Hanling et Daniel S. Roche. – Linear algebra-based proof of retrievability protocol for ensuring data integrity, juillet 2021. 5 kSLOC.

[S141] The LINBOX group. – LINBOX 1.7.0 Sablet. – Debian (`liblinbox, liblinbox-dev`), décembre 2021. 152 kSLOC.

[S142] Jean-Guillaume Dumas et Burak Ekici. – CoqEffects: Certified proofs in programs involving side-effects, 2013. 28 kSLOC.

[S143] Christophe Chabot, Jean-Guillaume Dumas, Laurent Fousse et Pascal Giorgi. – Recint: Recursive fixed precision integers, 2011. 7 kSLOC.

[S144] Brice Boyer et Jean-Guillaume Dumas. – FFSpMv: Finite field sparse matrix-vector product on multi-cores, 2010. 43 kSLOC.

[S145] Brice Boyer et Jean-Guillaume Dumas. – Galet: Matrix multiplication schedule generator, janvier 2009. 11 kSLOC.

[S146] Jean-Guillaume Dumas et Clément Pernet. – Exact linear system resolution in M4RI, novembre 2008.

[S147] Aude Rondepierre et Jean-Guillaume Dumas. – Hybrid optimal control, 2005. 7 kSLOC.

[S148] 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

[T149] Jean-Guillaume Dumas et Bruno Grenet. – ***Fast in-place accumulation***. – Rapport technique, IMAG-hal-05000159, arXiV cs.SC/2503.xxxxx, mars 2025.

[T150] Jean-Guillaume Dumas, Clément Pernet et Alexandre Sedoglavic. – ***Towards automated generation of fast and accurate algorithms for recursive matrix multiplication***. – Rapport technique, IMAG-hal-04995684, arXiV cs.SC/2503.xxxxx, mars 2025.

[T151] Jean-Guillaume Dumas, Sonia Jimenez-Garces, Mathis Mourey et Florentina Şoiman. – ***The forking effect***. – Rapport technique, IMAG-hal-03216121, arXiV cs.CR/2307.11718, mai 2021.

[T152] Jean-Guillaume Dumas. – ***Contributions au calcul exact intensif***. – Habilitation à diriger des recherches en Informatique et mathématiques appliquées, Université de Grenoble, 20 juillet 2010.

[T153] 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. Gaspard Anthoine ; 2. Benoît Badrignans ; 3. Alexandre Berzati ; 4. Pascal Bouvry ; 5. Brice Boyer ; 6. Alexis Breust ; 7. Xavier Bultel ; 8. Christophe Chabot ; 9. Van-Dat Cung ; 10. Vincent Danjean ; 11. Jannik Dreier ; 12. Jacques Dubrois ; 13. Cécile Dumas-Canovas ; 14. Dominique Duval ; 15. Burak Ekici ; 16. Philippe Elbaz-Vincent ; 17. Laurent Fousse ; 18. Alexis Galan ; 19. Thierry Gautier ; 20. Mark W. Giesbrecht ; 21. Roland Gillard ; 22. Pascal Giorgi ; 23. Louis Goubin ; 24. Rod Gow ; 25. Bruno

Grenet ; 26. Mike Hanling ; 27. Frank Heckenbach ; 28. Joris van der Hoeven ; 29. Hicham Hossayni ; 30. Bradford Hovinen ; 31. Guillaume Huard ; 32. Sonia Jimenez Garces ; 33. Mélanie de Jonghe ; 34. Hugo Jonker ; 35. Erich L. Kaltofen ; 36. Pascal Lafourcade ; 37. Franck Leprévost ; 38. Julio Ernesto López Fenner ; 39. David Lucas ; 40. Sabine Machenaud ; 41. Aude Maignan ; 42. Gary McGuire ; 43. Francis Melemedjian ; 44. Daiki Miyahara ; 45. Takaaki Mizuki ; 46. Mathis Mourey ; 47. Atsuki Nagao ; 48. Grégory Nuel ; 49. Jean-Baptiste Orfila ; 50. Clément Pernet ; 51. Victor Y. Pan ; 52. Florian Pebay-Peyroula ; 53. François Pebay-Peyroula ; 54. Marie-Laure Potet ; 55. Damien Pous ; 56. Maxime Puys ; 57. Bruno Raffin ; 58. Christophe Rapine ; 59. Patrick Redon ; 60. Jean-Claude Reynaud ; 61. Jean-Luc Richier ; 62. Léo Robert ; 63. Jean-Louis Roch ; 64. Daniel S. Roche ; 65. Aude Rondepierre ; 66. Étienne Roudeix ; 67. Bruno Salvy ; 68. B. David Saunders ; 69. Valentin Savin ; 70. Tatsuya Sasaki ; 71. Alexandre Sedoglavic ; 72. John Sheekey ; 73. Kazumasa Shinagawa ; 74. Florentina Şoiman ; 75. Hideaki Sone ; 76. Ziad Sultan ; 77. Éric Tannier ; 78. Emmanuel Thomé ; 79. Pascal Thoniel ; 80. Ariane Tichit ; 81. Denis Trystram ; 82. Will J. Turner ; 83. Anna Urbańska ; 84. Sébastien Varrette ; 85. Gilles Villard ; 86. Zhendong Wan ; 87. Volkmar Welker ; 88. Lihong Zhi ; 89. Wei Zhou ; 90. Vincent Zucca.

RÉFÉRENCES

[154 - Arreche (2018)] Carlos Arreche (éditeur). – ***ISSAC'2018, Proceedings of the 2018 International Symposium on Symbolic and Algebraic Computation, New York, USA***, 16–19 juillet 2018. – ACM Press, New York.

[155 - Chen (2024)] Shaoshi Chen (éditeur). – ***ISSAC'2024, Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation, Raleigh, NC-USA***, 16–19 juillet 2024. – ACM Press, New York.

[156 - Gao (2016)] Xiao-Shan Gao (éditeur). – ***ISSAC'2016, Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation, Waterloo, ON, Canada***, 20–22 juillet 2016. – ACM Press, New York.

[157 - Gutierrez (2004)] Jaime Gutierrez (éditeur). – ***ISSAC'2004, Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, Santander, Spain***, 4–7 juillet 2004. – ACM Press, New York.

[158 - Jeffrey (2008)] David Jeffrey (éditeur). – ***ISSAC'2008, Proceedings of the 2008 International Symposium on Symbolic and Algebraic Computation, Hagenberg, Austria***, 20–23 juillet 2008. – ACM Press, New York.

[159 - Kauers (2005)] Manuel Kauers (éditeur). – ***ISSAC'2005, Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, Beijing, China***, 24–27 juillet 2005. – ACM Press, New York.

[160 - Kauers (2013)] Manuel Kauers (éditeur). – ***ISSAC'2013, Proceedings of the 2013 International Symposium on Symbolic and Algebraic Computation, Boston, USA***, 26–29 juin 2013. – ACM Press, New York.

[161 - Kauers (2019)] Manuel Kauers (éditeur). – ***ISSAC'2019, Proceedings of the 2019 International Symposium on Symbolic and Algebraic Computation, Beijing, China***, 15–18 juillet 2019. – ACM Press, New York.

[162 - Leykin (2020)] Anton Leykin (éditeur). – ***ISSAC'2020, Proceedings of the 2020 International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece***, 20–23 juillet 2020. – ACM Press, New York.

[163 - May (2009)] John P. May (éditeur). – ***ISSAC'2009, Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation, Seoul, Korea***, 28–31 juillet 2009. – ACM Press, New York.

[164 - Mora (2002)] Teo Mora (éditeur). – ***ISSAC'2002, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Lille, France***, 7–10 juillet 2002. – ACM Press, New York.

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

[166 - Nabeshima (2014)] Katsusuke Nabeshima (éditeur). – ***ISSAC'2014, Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, Kobe, Japan***, 23–25 juillet 2014. – ACM Press, New York.

[167 - Safey El Din (2017)] Mohab Safey El Din (éditeur). – ***ISSAC'2017, Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation, Kaiserslautern, Germany***, 25–28 juillet 2017. – ACM Press, New York.

[168 - Traverso (2000)] Carlo Traverso (éditeur). – ***ISSAC'2000, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, Saint-Andrews, Scotland***, 6–9 août 2000. – ACM Press, New York.

[169 - Yokoyama (2015)] Kazuhiro Yokoyama (éditeur). – ***ISSAC'2015, Proceedings of the 2015 International Symposium on Symbolic and Algebraic Computation, Bath, UK***, 6–10 juillet 2015. – ACM Press, New York.