CURRICULUM VITAE (Version 17/04/23)

• Nom : **BALLET**

• Prénom : **Stéphane**

• Date et lieu de naissance : 7 janvier 1971 à Valence (26)

• Marié, deux enfants.

• Email: stephane.ballet@univ-amu.fr .

• Fonction et établissement actuel :

Maître de Conférences en Mathématiques HC (section 25) à l'Université d'Aix-Marseille, Faculté des Sciences, Département de Mathématiques, Institut de Mathématiques de Marseille (I2M).

• Diplomes principaux: **Habilitation à Diriger des Recherches en Mathématiques, Doctorat en Mathématiques, DEA d'Informatique et Mathématiques, Diplomé de l'Ecole Internationale des Sciences du Traitement de l'Information (EISTI), Master en Philosophie (spécialité: Histoire et Philosophie des Sciences Fondamentales (Mathématiques et Physique))**.

• Qualifications : **qualifié** aux fonctions de Professeur des Universités **en section 25** (Mathématiques) depuis 2007, aux fonctions de Professeur des Universités **en section 26** (Mathématiques appliquées et applications des Mathématiques) depuis 2015, **qualifié** aux fonctions de Maître de Conférences des Universités **en section 25** (Mathématiques) et **en section 27** (Informatique) en 1999.

• Distinctions : **Vice-président de la Société Mathématique de France** (en cours depuis juin 2020), lauréat de la **Prime d'Encadrement Doctoral et de Recherche (PEDR)** attribuée par l'Université d'Aix-Marseille pour les périodes (2021-2025, 2018-2021), **Lettre de remerciement** (datée du 21/06/2016) du Département de Géographie de l'Université Blaise-Pascal (Clermont Ferrand), lauréat de la **Prime d'Excellence Scientifique (PES)** attribuée par l'Université d'Aix-Marseille pour la période 2014-2017, de la **PES** attribuée par l'Université de la Méditerranée pour la période 2009-2013, d'une **Bonification d'ancienneté** d'un an pour mobilité géographique (de plus d'un an en dehors de l'espace européen) en mars 2010, de la **PEDR** attribuée par le Ministère pour la période 2004-2008 et d'un **Congé pour Recherche (CRCT)** au titre de l'établissement Université de Polynésie Française d'une valeur d'un semestre (sur un total d'un semestre attribué à l'établissement) pour la période 2005-2006, Médaille de Bronze de la Défense Nationale (1996).

• Nombre de Publications : **43 publications internationales.**

• Nombre de Publications (4 dernières années) : **10 publications internationales.**

Formation

1) **Formations principales et diplomantes:**

• Juin 2014: **Master (Recherche) de Philosophie** (Master 2) (spécialité: Histoire et Philosophie des Sciences Fondamentales (Mathématiques et Physique)), mention Très Bien.
Mémoire : *Sur la nature de l'espace à partir de la conception d'Einstein - L'argument du trou et Paradoxe d'Einstein-Podolsky-Rosen*, au Centre d'EPistémologie et d'ERgologie Comparative et Centre de Physique Theorique (CPT) de l'Université d'Aix-Marseille sous la direction de Eric Audureau et Thierry Masson.

• Juin 2013: **Maitrise de Philosophie** (Master 1) (spécialité: Histoire et Philosophie des Sciences Fondamentales (Mathématiques et Physique)), mention Bien.

• 26 juin 2006: **Habilitation à Diriger des Recherches**, spécialité Mathématiques, Faculté des Sciences de Luminy, Université de la Méditerranée (Aix-Marseille II).

Titre: *Corps de fonctions algébriques et application à l'étude de la complexité bilinéaire de la multiplication dans les corps finis.*

Jury: Gilles Lachaud (D.R. CNRS/Marseille), Philippe Langevin (Prof. Université du Sud Toulon-Var), Robert Rolland (HDR, Université de la Méditerranée), Reynald Lercier (HDR, DGA/Rennes), Igor Shparlinski (Prof. Université Macquarie Sydney Australie), Patrick Solé (D.R. CNRS/Nice).

• 1998-1999: **Etudes Post-Doctorales** au Centre d'Electronique de l'Armement, Division Centre de l'Armement pour la Sécurité des Systèmes d'Information (CASSI), Cellule Etudes Cryptographiques (EC), à Bruz (35).

• 01/09/96-02/11/98: **Thèse de Doctorat de l'Université**, spécialité Mathématiques Discrètes et Fondements de l'Informatique, Faculté des Sciences de Luminy, Université de la Méditerranée (Aix-Marseille II), Mention Très Honorable, sous la direction de Robert Rolland. **Allocataire de recherche (DGA/CNRS)** de l'Institut de Mathématiques de Luminy (CNRS UPR 9016).

Titre: *Etude de la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques.*

Jury: Jean-Marc Couveignes (Prof.), Gilles Lachaud (D.R.), Ruud Pellikaan (Prof. Pays-Bas), François Rodier (D.R.), Robert Rolland (HDR,), Michael Tsfasman (D.R. Russie), Serguei Vladut (Prof.), Jacques Wolfmann (Prof.).

• 1994-95: **DEA d'Informatique et Mathématiques**, Faculté des Sciences de Luminy, Université de la Méditerranée (Aix-Marseille II), Mention Bien.
Mémoire : *Evaluation du groupe d'automorphismes vectoriels fixant les classes modulo un groupe cyclique*, au Groupe d'Etude du Codage de Toulon sous la direction de Jacques Wolfmann et Philippe Langevin.

• 1991-94: **Ecole Internationale des Sciences du Traitement de l'Information** (E.I.S.T.I) à Cergy-Pontoise (95).

• 1989-91: **Classes Préparatoires aux Grandes Ecoles** préparées au Lycée Militaire d'Aix en Provence - Obtention du **DEUG A des Sciences et Structure de la Matière** - Admis à l'E.I.S.T.I.

2) **Formations complémentaires:**

• **Formation AMU** (30/09/2022), **CIPE**: *Sensibilisation à la lutte contre les extrémismes, les racismes, l'antisémitisme et les discriminations.*

Objectifs:

-Découverte de l'histoire du Camp des Milles.

- Replacer la question du racisme dans une histoire longue afin de comprendre les mécanismes à l'œuvre dans la société.

Programme

- Visite commentée du Site-mémorial du Camp des Milles, Visite des lieux d'internement et de déportation.

- Compréhension des dynamiques conduisant aux discriminations et celles permettant d'y résister. Apports théoriques et cas d'études.

• **Formation AMU** (07/06/2022 et 14/06/2022), **CIPE**: *Apprendre à apprendre: utiliser les sciences cognitives pour faciliter l'apprentissage des étudiants.*

- Comprendre l'apport des sciences cognitives dans l'apprentissage des étudiants et dans sa propre pratique pédagogique.

- Se former à l'enseignement de trois cours magistraux reposant sur un certain nombre de concepts fondateurs en sciences cognitives bénéfique aux apprentissages des étudiants.

- mettre en perspective l'apport des contenus présentés pour réfléchir et développer des TD appropriés aux différentes formations disciplinaires.

• **Formation AMU** (24/05/2022), **CIPE'Lab**: *Développer la réflexivité des étudiants: pourquoi et comment?*

- Identifier la réflexivité et les stratégies réflexives interactives.

- Représenter l'impact d'une pratique réflexive dans le parcours des étudiants, notamment en termes d'autonomie et de régulation des apprentissages vers la réussite.

- Découvrir les situations qui permettent aux étudiants d'être réflexifs.

- Adapter sa pratique pour favoriser la réflexivité des étudiants.

Expériences professionnelles

• Depuis le 1er septembre 2014: **Maître de Conférences Hors-classe en Mathématiques (section 25)** par la voie nationale (CNU).

• Depuis le 1er janvier 2012: **Maître de Conférences en Mathématiques (section 25)** à l'**Université d'Aix-Marseille**, Faculté des Sciences, Département de Mathématiques, **Institut de Mathématiques de Marseille (I2M, CNRS UMR 8080)** (Institut de Mathématiques de Luminy (CNRS FRE 3529) jusqu'au 1er janvier 2014) équipe **Arithmétique et Théorie de l'Information**, à Marseille (13).

• 1er février 2008 - 1er janvier 2012: **Maître de Conférences en Mathématiques (section 25)** à l'**Université de la Méditerranée** (Aix-Marseille II, Faculté des Sciences de Luminy, Département de Mathématiques), **Institut de Mathématiques de Luminy (CNRS UMR 6206)**, équipe **Arithmétique et Théorie de l'Information**, à Marseille (13).

• 1er février 2001 - 1er février 2008: **Maître de Conférences en Mathématiques (section 25)** à l'Université de la Polynésie Française, Laboratoire de **Géométrie Algébrique**

et Applications à la Théorie de l'Information (EA 3893 GAATI), en Polynésie Française (TOM).

• 1er septembre 1999 - 31 janvier 2001: **Enseignant-Chercheur Contractuel en Informatique** au **Centre de Recherche des Ecoles Militaires de Saint Cyr Coëtquidan (CREC)**, à Guer (56).

• **1er septembre 1997- 31 août 1999: recherche et vacations de mathématiques dans l'enseignement supérieur** à l'Université de la Méditerranée (1er cycle, 179 heures), à Marseille (13) et au Centre d'Electronique de l'Armement (3ème cycle, 32 heures), à Bruz (56).

• 1995-96: **Service National** au Lycée Militaire d'Aix En Provence: chargé des études surveillées (aide aux devoirs) et de l'internat des élèves de seconde.

Activités d'enseignement

1) Troisième cycle universitaire:

• **Depuis le 1er septembre 2012: Cours de mathématiques** à l'Université d'Aix-Marseille (AMU)

Cours doctoraux (ED 144): cours transverse aux doctorants de mathématiques et d'informatique: *Histoire de la pensée scientifique* (24 h, 2022-2023)

Master 2 Recherche Mathématiques Fondamentales : *Géométrie algébrique et arithmétique* (2019-2020):

Courbes algébriques et elliptiques (tronc commun) (27 heures).

Master 2 Recherche Mathématiques Discrètes et Fondements de l'Informatique:

Algèbre, Arithmétique et Codage (tronc commun) (36 heures).

Introduction aux courbes elliptiques et à la cryptographie elliptique (tronc commun) (18 heures).

Courbes et corps de fonctions algébriques (tronc commun) (36 heures).

• **1er février 2008 - 1er septembre 2012: Cours de mathématiques** à l'Université de la Méditerranée

Master 2 Recherche Mathématiques Discrètes et Fondements de l'Informatique :

Courbes et corps de fonctions algébriques (tronc commun) (36 heures).

Master 2 Pro Mathématiques et Informatique des Nouvelles Technologies :

Cryptographie(tronc commun) (108 heures).
Cryptographie(option) (18 heures).

• **Août 2003: Cours de Mathématiques Effectives** à l'Ecole CIMPA-UNESCO MEXIQUE (Centre International de Mathématiques Pures et Appliquées): Arithmétique, algèbre commutative, géométrie algébrique et applications, en laison avec le calcul formel.

Introduction à la géométrie algébrique des courbes - Application en kash (7,5 heures): cours de mathématiques de niveau 3ème cycle aux doctorants de la zone Amérique du Sud.

• **1er janvier 1999- 31 juillet 1999: Cours de mathématiques** au Centre d'Electronique de l'Armement (32 heures).

Introduction à la théorie des corps de fonctions algébriques en une variable (32 heures): cours de mathématiques de niveau 3ème cycle aux chercheurs de l'équipe Etudes Cryptographiques de la division Sécurité des Systèmes d'Information.

2) Second cycle universitaire:

• **Depuis le 1er septembre 2012: Cours de mathématiques** à l'Université d'Aix-Marseille (AMU)

Master 1 Mathématiques et Applications: Algèbre et Géométrie (Théorie des groupe et Théorie de Galois) (48 heures).

Master 1 Mathématiques et Applications: Algèbre (Théorie de Galois) (216 heures).

Master 1 Mathématiques et Applications: Algèbre et Arithmétique (72 heures).

Licence 3ème année: Histoire et épistémologie des mathématiques (72 heures).

Licence 3ème année: Histoire des sciences (108 heures).

Licence 3ème année: Structures Algébriques (216 heures).

Licence 3ème année: Géométrie Affine et Euclidienne (216 heures).

Mission à l'UPF (Avril-Mai 2022): Arithmétique des Anneaux et des Corps (Licence 3ème année; 37,5 heures).

Mission à l'UPF (Avril 2017): Anneaux et des Corps (Licence 3ème année; 37,5 heures).

Mission à l'UPF (Avril 2016): Géométrie (Licence 3ème année; 37,5 heures).

Ecole d'Ingénieurs Universitaire de Polytech Marseille (Luminy) (Filière HUGO: Formation en alternance de personnes en situation de handicap pour le diplôme d'Ingénieur en informatique): Optimisation et Recherche opérationnelle (3ème année): 27 heures (2018, 1ère promotion).

• **1er février 2008 - 1er septembre 2012: Cours de mathématiques** à l'Université de la Méditerranée

Master 1 Mathématiques et Applications: Algèbre (Théories de groupes et des anneaux) (142 heures).

Master 1 Mathématiques et Applications: Compléments de mathématiques pour les concours (Préparation Capes et Agrégation) (330 heures).

Licence 3ème année: Analyse numérique (216 heures).

Licence 3ème année: Algèbre générale (66 heures).

Ecole Supérieure d'Ingénieurs de Luminy (ESIL/IRM):
option Systèmes Informatiques Critiques et Applications 2ème année, cours Fondements Protocoles Cryptographiques: Complexité algorithmique (15 heures).

option Systèmes Informatiques Critiques et Applications 3ème année, cours Cryptographie avancée : Courbes elliptiques et applications à la cryptographie (30 heures).

Mission à l'UPF (Avril 2010): Géométrie (Licence 3ème année; 37,5 heures).

• **1er février 2001 - juillet 2007: Cours de mathématiques** à l'Université de la Polynésie Française, à l'IUFM du Pacifique et pour la Direction de l'Enseignement Secondaire de la Polynésie Française (DES).

IUFM : Préparation Capes (67,5 heures)

DES: Préparation Agrégation Interne

Licence 3ème année: TD d'Algèbre-Arithmétique (194,5 heures)

Licence 3ème année: Cours de Géométrie (120 heures)

Licence 3ème année: TD de Calcul Intégral (242 heures)

Licence 3ème année: Cours d'histoire des mathématiques (4 heures)

• **1er septembre 1999 - 31 janvier 2001: Cours d'informatique** aux Ecoles Militaires de Saint Cyr Coëtquidan.

Algorithmique avancée (langage d'application: C) (Cours et TD : 160 heures): 2ème année de l'Ecole Spéciale Militaire de Saint Cyr Coëtquidan (Ecole d'Ingénieur).

Base de données - Analyse (Merise) et Conception (Access) (Cours et TD: 52 heures): élèves officiés de l'Ecole Militaire du Corps Technique de l'Administration (niveau licence).

3) Premier cycle universitaire:

• **Depuis le 1er septembre 2012: Cours de mathématiques** à l'Université d'Aix-Marseille (AMU)

Licence 2ème année : Géométrie 1 (72 heures)

Licence 1ère année MIASH: Fonctions d'une ou deux variables (52,5 heures)

Licence 2ème année : Analyse 2 (216 heures)

Licence 2ème année : Probabilités et Statistique 1 (228 heures)

Licence 1ère année MIASH: Eléments d'analyse (228 heures)

• **1er février 2008 - 1er septembre 2012: Cours de mathématiques** à l'Université de la Méditerranée

Licence 2ème année: colles d'algèbre et d'analyse (44 heures)

Licence 1ère année: colles de Maths Discrètes (10 heures)

• **1er février 2001 - juin 2007: Cours de mathématiques** à l'Université de la Polynésie Française.

Licence 2ème année: TD d'algèbre approfondie (54 heures)

Licence 2ème année: TD d'analyse (84 heures)

DEUG MIAS 2ème année: Cours d'algèbre (100 heures)

DEUG SM 2ème année: Cours d'algèbre-analyse (72 heures)

Licence 1ère année: TD d'algèbre (36 heures)

DEUG MIAS 1ère année: TD d'algèbre-analyse (275,5 heures)

• **1er septembre 1999 - 31 janvier 2001: Cours d'informatique** aux Ecoles Militaires de Saint Cyr Coëtquidan.

Algorithmique et calcul formel (langages d'application: Pascal et Mathematica) (Cours et TD : 160 heures) : préparation de l'épreuve du DEUG de Sciences (Rennes I) pour les élèves officiers de 2ème année de l'Ecole Militaire Interarmes (EMIA).

• **1er septembre 1997- décembre 1998: vacations de mathématiques dans l'enseignement supérieur** à l'Université de la Méditerranée (1er cycle, 179 heures).

DEUG SM, MIAS, MASS 2ème année: TD Mathématiques de base (120 heures)+ Colles Mathématiques avancées (35 heures)

DEUG SM, MIAS, MASS 1ère année: TD algèbre linéaire et géométrie (24 heures)

4) Enseignement secondaire et école primaire:

• **Depuis le 1er février 2008:**

IREM (Marseille):

Stages Hypocampe (initiation à la recherche dans le cadre de la liaison Lycée/Université):

- mai 2022: stage Fractal (classes de 2nde et 1ère): tuteur (12 heures). J'ai proposé de tester une expérience pédagogique nouvelle pour les stages hypocampe: proposer un thème d'Histoire des mathématiques. Dans ce cadre, j'ai pris en charge un groupe sur le thème de l'Histoire des fractales. J'ai eu en charge la clôture du stage avec débriefing.

- novembre 2008, 2009, 2010: stages Codage dans la vie courante (classes: 1ère S et Terminale S): responsable (72 heures).

- mai 2008: stage Arithmétique (classes de 2nde): tuteur (12 heures).

Journées Futurs Bacheliers (2009): co-présentation de l'Irem (12 heures).

• **Janvier 1999 - juin 2000:** Membre bénévole de l'association Espoir et Entraide Scolaire à Rennes, études surveillées d'élèves de l'école primaire et du collège, de janvier 1999 à juin 2000.

• **1er septembre 1995 - 31 août 1996:** Service National en tant que répétiteur au Lycée Militaire d'Aix en Provence, chargé des études surveillées (aide aux devoirs) et de l'internat des élèves de seconde.

Activités de recherche

Mon domaine de recherche concerne la géométrie algébrique et l'arithmétique des courbes et leurs applications en théorie de l'information (codage correcteurs d'erreurs, cryptographie, algorithmique).

Mes travaux de spécialité concernent la géométrie algébrique, l'algèbre et l'arithmétique des variétés sur les corps finis et leurs applications en théorie de l'information (codage correcteurs d'erreurs, cryptographie, algorithmique):

1) Etude de la complexité bilinéaire de la multiplication, et récemment de la complexité multilinéaire de la k-multiplication, dans les corps finis: détermination de rang de tenseur de la multiplication et de la k-multiplicationpar interpolation sur des courbes algébriques. Des applications directes de ces travaux concernent l'algorithmique dans les corps finis, la cryptographie, et la théorie des codes correcteurs d'erreurs.
2) La construction effective d'algorithmes de multiplication dans les corps finis par interpolation sur des courbes de genre quelconque.
3) La construction (et la descente du corps de définition) de tours (et plus généralement de suites) de corps de fonctions définis sur des corps finis (tours de type Kummer, Artin-Schreier, modulaires, Shimura, modules de Drinfeld), plus denses que celles de Garcia-Stichtenoth.
4) Etude des diviseurs non-spéciaux de degré g et $g-1$ d'un corps de fonctions algébriques de genre g défini sur un corps fini.
5) Etude des diviseurs de dimension zéro d'un corps de fonctions algébriques de genre g défini sur un corps fini.
6) Etude du nombre de classes d'un corps de fonctions algébriques de genre g défini sur un corps fini.
7) Etude du théorème de Yao pour les générateurs pseudo-aléatoires.
8) Etude des codes de Reed-Muller.

Autres travaux

Ces quatre dernières années, j'ai fourni un effort pour investir mes connaissances mathématiques dans des thématiques transdisciplinaires ou dans d'autres disciplines. En particulier, j'ai effectué des travaux de recherche dans deux directions:

1) J'ai participé à des travaux de recherche en Géographie Physique, faisant appel à des connaissances en sciences du traitement de l'information (statistique, analyse de données etc...), ce qui a donné lieu à deux publications internationales ainsi qu'à un poster présenté en Conférence Internationale.

2) J'ai écrit un mémoire de recherche de niveau Master 2 en Histoire et Philosophie des Sciences Fondamentales sur *le Paradoxe du trou et le Paradoxe d'Einstein-Podolski-Rosen*, dans lesquels la notion de rang de tenseur joue un rôle.

Publications et travaux

1) Publications dans une revue internationale avec comité de lecture international:

a) Publications dans le domaine de spécialité

• *Construction of asymmetric Chudnovsky-type algorithms for multiplication in finite fields*, co-écrit avec N. Baudru, A. Bonnecaze, M. Tukumuli, Designs, Codes and Cryptography, vol. 90, no. 12, 2783-2811, 2022.

• *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, co-écrit avec A. Bonnecaze et T.-H. Dang, Cryptography and Communications, Cryptography and Communications, 13 (4), 495-517, 2021.

• *On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry*, co-écrit avec J. Chaumine, J. Pieltant, M. Rambaud, H. Randriambololona et R. Rolland, Uspekhi Matematicheskikh Nauk (Russian Mathematical Surveys), 76:1(457), 31–94, 2021.

• *Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields*, co-écrit avec A. Zykin, Designs, Codes and Cryptography, 87 (no 2-3), 17-52, 2019.

• *Tower of algebraic function fields with maximal Hasse-Witt invariant and tensor rank of multiplication in any extension of $\mathbb{F}_2$ and $\mathbb{F}_3$*, co-écrit avec Julia Pieltant, Journal of Pure and Applied Algebra, volume 222, 1069–1086, 2018.

• *Arithmetic in finite fields based on Chudnovsky Multiplication algorithm*, co-écrit avec K. Atighehchi, A. Bonnecaze, et R. Rolland, Mathematics of Computation, volume 86, no. 308, 2975–3000, 2017.

• *On the construction of elliptic Chudnovsky algorithms for multiplication in large extensions of finite fields*, co-écrit avec Alexis Bonnecaze et Mila Tukumuli, Journal of Algebra and its Applications, volume 15, number 1, 26 pages, 2016.

• *Effective bounds on class number and estimation for any step of towers of algebraic function fields over finite fields*, co-écrit avec R. Rolland et Seher Tutdere, Moscow Mathematical Journal, volume 15, number 4, 653-677, October–December 2015.

• *Lower bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers*, co-écrit avec R. Rolland et Seher Tutdere, Moscow Mathematical Journal, volume 15, number 3, 425–433, July-September 2015.

• *On low weight codewords of generalized affine and projective Reed-Muller codes*, co-écrit avec Robert Rolland, Designs, Codes and Cryptography, 70 (1-2), 2014.

• *Lower bounds for the class number of algebraic function fields defined over a finite field*, co-écrit avec R. Rolland, Journal de Théorie des Nombres de Bordeaux, 24, 505-540, 2012.

• *A note on Yao's theorem about pseudo-random generators*, co-écrit avec R. Rolland, Cryptography and Communications: Volume 3, Issue 4, 189–206, 2011.

• *On the tensor rank of multiplication in any extension of* $\mathbb{F}_2$, co-écrit avec J. Pieltant, Journal of Complexity 27 (2011), pp. 230-245.

• *On the existence of dimension zero divisors in algebraic function fields defined over* $\mathbb{F}_q$, co-écrit avec C. Ritzenthaler et R. Rolland, Acta Arithmetica, 143 (2010), 4, 377-392.

• *On the tensor rank of the multiplication in the finite fields*, Journal of Number Theory, 128 (2008), 1795-1806.

• *An improvement of the construction of the D.V. and G.V. Chudnovsky algorithm for multiplication in finite fields*, Theoretical Computer Science, 352 (2006), 293-305.

• *On the existence of non-special divisors of degree* g *and* $g-1$ *in algebraic function fields over* $\mathbb{F}_q$, co-écrit avec Dominique Le Brigand, Journal of Number Theory, 116 (2006), 293-310.

• *On the bounds of the bilinear complexity of multiplication in some finite fields*, co-écrit avec Jean Chaumine, Applicable Algebra in Engineering, Communication and Computing, 15 (2004), 205-211.

• *Multiplication algorithm in a finite field and tensor rank of the multiplication*, Co-écrit avec Robert Rolland, Journal of Algebra, 272/1 (2004), 173-185.

• *Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of* $\mathbb{F}_q$, Finite Fields and Their Applications, 9 (2003), 472-478.

• *Quasi-optimal algorithms for multiplication in the extensions of* $\mathbb{F}_{16}$ *of degree 13, 14 and 15*, Journal of Pure and Applied Algebra, 171 (2002), 149-164.

• *Curves with many points and multiplication complexity in any extension of* $\mathbb{F}_q$, Finite Fields and Their Applications, 5 (1999), 364-377.

En préparation ou révision:

• *Multiplication in finite fields with Chudnovsky-type algorithms on the projective line*, co-écrit avec A. Bonnecaze et B. Pacifico.

b) Publications hors-spécialité ou transdisciplinaires

• *Persistence at the final stage of volcanic island ontogeny: abiotic predictors explain native plant species richness on 111 remote Pacific Atolls*, Sébastien Larrue, Jean-François Butaud, Curtis Daehler, Stéphane Ballet, Julien Chadeyron, Roger Oyono, Ecology and Evolution, 8(25), 2018.

• *Native plant species richness on Eastern Polynesia's remote atolls: Which abiotic factors influence its spatial pattern?*, Sébastien Larrue, Jean-François Butaud, Pascal Dumas, et Stéphane Ballet, Progress in Physical Geography, 40 : 112-134, 2015.

En préparation:

• *At the final volcanic island ontogeny: An index to predict native plant species richness*, Sébastien Larrue, Jean-François Butaud, Curtis Daehler, Stéphane Ballet, Julien Chadeyron and Roger Oyono.

2) Notes aux Comptes Rendus de l'Académie des Sciences (CRAS):

• *On the Construction of the Asymmetric Chudnovsky Multiplication Algorithm in Finite Fields Without Derivated Evaluation*, co-écrit avec N. Baudru, A. Bonnecaze, M. Tukumuli, C. R. Acad. Sci. Paris, Ser. I 355 (2017) 729–733.

• *Effective arithmetic in finite fields based on Chudnovsky multiplication algorithm*, co-écrit avec K. Atighehchi, A. Bonnecaze, et R. Rolland, C. R. Acad. Sci. Paris, Mathématique 354 (2016), pp. 137-141.

• *Minoration du nombre de classes d'un corps de fonctions algébriques défini sur un corps fini*, co-écrit avec R. Rolland, C. R. Acad. Sci. Paris, Ser. I 349, 709–712, 2011.

• *Amélioration des bornes de la complexité bilinéaire de la multiplication dans certains corps finis* , co-écrit avec Jean Chaumine, C. R. Acad. Sci. Paris, Théorie des nombres, Ser. I 339 (2004), 383-385.

3) Actes dans un colloque international avec comité de lecture :

• *Chudnovsky-type algorithms over the projective line using generalized evaluation maps*, co-écrit avec B. Pacifico, 4th International Conference on Codes, Cryptology and Information Security (C2SI 2023, Rabat, Marocco, May 29-31,2023), Lecture Notes in Computer Science, vol. , Springer, Cham, 2023, à paraître.

• *Chaining Multiplications in Finite Fields with Chudnovsky-type Algorithms and Tensor Rank of the k-multiplication*, co-écrit avec Robert Rolland, In: Poulakis, D., Rahonis, G. (eds) Algebraic Informatics. Conference in Algebraic Informatics (CAI 2022). Lecture Notes in Computer Science, vol 13706, Springer, Cham, 2022.

• *Polynomial constructions of Chudnovsky-type algorithms for multiplication in finite fields with linear bilinear complexity*, S. Ballet, A. Bonnecaze, et B. Pacifico, International Workshop on Arithmetic of Finite Field (WAIFI 2022, Chengdu, China, August 29-September 2, 2022), Lecture Notes in Computer Science, à paraître.

• *A strategy to optimize the complexity of Chudnovsky-type algorithms over the projective.* co-écrit avec A. Bonnecaze et B. Pacifico, *18th International Conference Arithmetic, Geometry, Cryptography and Coding Theory (June 10-14, 2021)*, Arithmetic, Geometry, Cryptography and Coding theory, Contemporary Mathematics, Volume 779, Amer. Math. Soc., 2022.

• *On the number of effective divisors in the algebraic function fields defined over a finite field*, co-écrit avec G. Lachaud et R. Rolland, *17th International Conference Arithmetic, Geometry, Cryptography and Coding Theory (June 10-14, 2019)*, Arithmetic, Geometry, Cryptography and Coding theory, Contemporary Mathematics, 770, Amer. Math. Soc., 29-49, 2021.

• *On the scalar complexity of Chudnovsky^2 multiplication algorithm in finite fields*, co-écrit avec A. Bonnecaze, T.-H. Dang, Proceedings International Conference on Algebraic Informatics (CAI 2019), Lecture Notes in Computer Science, LNCS 11545 , 64-75, 2019.

• *On some bounds for symmetric tensor rank of multiplication in finite fields*, co-écrit avec J. Pieltant, M. Rambaud et J. Sijsling, *15th International Conference Arithmetic, Geometry, Cryptography and Coding Theory (May 18-22, 2015)*, Arithmetic, Geometry,

Cryptography and Coding theory, 93-121, Contemporary Mathematics, 686, Amer. Math. Soc., Providence, RI, 2017.

• *Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field*, co-écrit avec Jean Chaumine and Julia Pieltant, Proceedings International Conference on Algebraic Informatics (CAI 2013), Lecture Notes in Computer Science, vol. 8080, 160-172, 2013.

• *Families of curves over any finite field attaining the generalized Drinfeld-Vladut bound*, co-écrit avec R. Rolland, Actes de la Conférence Internationale "Théorie des Nombres et Applications" (CIRM), Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr. 5-18, 2011.

• *On an application of the definition field descent of a tower of function fields* co-écrit avec Dominique Le Brigand et Robert Rolland, Colloque International Arithmetic, Geometry and Coding Theory 2005 (AGCT 10), Société Mathématique de France, sér. Séminaires et Congrès 21, 187–203, 2010.

• *A note on the tensor rank of the multiplication in the finite fields*, Proceedings of Symposium of Algebraic Geometry and Applications, Tahiti, 7-11 mai 2007. In J. Hirschfeld and J. Chaumine and R. Rolland, editors, Algebraic geometry and its applications, volume 5 of Number Theory and Its Applications, World Scientific (2008), 332-342.

• *On the bilinear complexity of the multiplication in finite fields*, co-écrit avec Robert Rolland, Arithmetic, Geometry and Coding Theory (AGCT 9), Société de Mathématiques de France, Séminaires et Congrés, 11 (2005), 179-188.

4) Livres ou édition d'actes :

• *17th International Conference Arithmetic, Geometry, Cryptography and Coding Theory (June 10-14, 2019)*, Stéphane Ballet, Gaetan Bisson and Irene Bouw (Eds), Contemporary Mathematics, 770, Amer. Math. Soc., 2021.

• *14th International Conference Arithmetic, Geometry, Cryptography and Coding Theory (June 3-7, 2013)*, Stéphane Ballet, Marc Perret and Alexey Zaytsev (Eds), Contemporary Mathematics, Vol. 637, 2014.

• *Special Issue on GEOCRYPT 2013*, S. Ballet, G. Bisson, R. Oyono, N. Theriault (Eds), Advances in Mathematics of Communications (AMC), Volume 8, Issue 4, 2014.

5) Communications orales ou affichée (poster) dans un colloque international avec comité de lecture:

a) Dans le domaine de spécialité

• *Chudnovsky-type algorithms over the projective line using generalized evaluation maps*, S. Ballet et Bastien Pacifico, 4th International Conference on Codes, Cryptology and Information Security (C2SI 2023), Rabat, Marocco, May 29-31 2023 (prévu).

• *Polynomial constructions of Chudnovsky-type algorithms for multiplication in finite fields with linear bilinear complexity*, B. Pacifico, S. Ballet et A. Bonnecaze, International Workshop on Arithmetic of Finite Field (WAIFI 2022), Chengdu, China, August 29-September 2, 2022.

• *Multiplication in finite fields with Chudnovsky-type algorithms over the projective line*, B. Pacifico, S. Ballet et A. Bonnecaze, WCC 2022: The Twelfth International Workshop on Coding and Cryptography, Universität Rostock (en visio), Allemagne, March 7 - March 11, 2021.

• *On the scalar complexity of Chudnovsky^2 multiplication algorithm in finite fields*, co-écrit avec A. Bonnecaze, T.-H. Dang, 8th International Conference on Algebraic Informatics (CAI 2019), Nis, Serbia, June 29-July 4, 2019.

• *Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields*, co-écrit avec A. Zykin, The Tenth International Workshop on Coding and Cryptography, Saint-Petersburg, Russia, September 18-22, 2017.

• Yet Another Conference on Cryptography (YACC 2016): *Effective arithmetic in finite fields based on Chudnovsky multiplication algorithm*, co-écrit avec K. Atighehchi, A. Bonnecaze et R. Rolland, IGESA Porquerolles, 6-10 juin 2016.

• *Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field*, co-écrit avec Jean Chaumine and Julia Pieltant, International Conference on Algebraic Informatics (CAI 2013), 2013.

• Colloque international Arithmetic, Geometry, Cryptography and Coding Theory (AGC^2T13), C.I.R.M (Marseille) : *Asymptotics for the class number of certain families of algebraic function fields defined over any finite field*, 14-18 mars 2011.

• Colloque international Workshop on tensors: *Tensor rank of the multiplication in finite fields*, co-écrit avec R. Rolland, Lab. J.A. Dieudonné, Département de Mathématiques, Université de Nice, 10-11-12 juin 2009.

• Colloque international Geometry and Cryptography (GEOCRYPT), Guadeloupe: *Asymptotically exact sequences of function fields and applications*, 27 avril - 1er mai 2009.

• Colloque international Geometry and Cryptography (GEOCRYPT), Guadeloupe: *Divisors of dimension zero*, co-écrit avec C. Ritzenthaler et R. Rolland, 27 avril - 1er mai 2009.

• Colloque international Journées Arithmétiques XXIV (Universités de Provence et de la Méditerranées, CNRS à Marseille) : *Application of the descent theory to the bilinear complexity of the multiplication in finite fields*, co-écrit avec Dominique Le Brigand et Robert Rolland, 4-8 juillet 2005.

• Colloque international Arithmetic, Geometry and Coding Theory (AGCT9), C.I.R.M (Marseille) : *Multiplication algorithm in a finite field and tensor rank of the multiplication*, co-écrit avec Robert Rolland, 19-23 mai 2003.

• *Bounds on the bilinear complexity of Multiplication in Any Extension of* $\mathbb{F}_q$, Proceedings of Workshop On Coding and Cryptography (INRIA WCC99), Paris, 11-14 janvier 1999.

• Colloque international Arithmetic, Geometry and Coding Theory (AGCT6), C.I.R.M (Marseille) : *On the complexity of multiplication in certain finite extensions of finite fields*, 23-27 juin 1997.

b) Hors-spécialité ou transdisciplinaire

• *Raised atoll and high volcanic island spatial pattern of native plant species richness on the atolls of Eastern Polynesia (French Polynesia, South Pacific Ocean)*, Sébastien Larrue, Jean-François Butaud, Pascal Dumas, et Stéphane Ballet, The 8th Biennial Conference of the International Biogeography Society, University of Arizona and the Tucson University Park, Tucson, Arizona, January 9-13, 2017.

6) Communications sur invitation en colloque ou séminaire international:

• *Dense families of modular curves, prime numbers and uniform symmetric tensor rank of multiplication in certain finite fields*, co-écrit avec A. Zykin,L-Functions and algebraic

varieties, International Conference in Memory of Alexey Zykin, Laboratory Poncelet and HSE, Independent University of Moscow, Russia, February 5-9, 2018 (Invited Speaker).

• International Workshop "Seminar on towers ", Sabanci university à Istambul (Turquie), Department of Mathematics: *Class number in algebraic function fields defined over finite fields and related problems*, février 2012.

• Seminar of Centre for Advanced Computing-Algorithms and Cryptography (ACAC), Department of Computing, Division of Information and Communication Sciences, Macquarie University, à Sydney (Australie):*Algebraic function fields and bilinear complexity of multiplication*, décembre 2006.

• Meeting Finite Fields: Theory and Applications, Oberwolfach (Allemagne), Quasi-optimal algorithms for multiplication in the extensions of $\mathbb{F}_{16}$ of degree 13, 14 and 15, 7–13 janvier 2001.

7) Communications sur invitation en colloque national:

• Les Rencontres Arithmétiques du GdR Informatique Mathématique GT Arith (RAIM 2022 : 13èmes Rencontres Arithmétique de l'Informatique Mathématique): *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 2-4 novembre 2022.

• Colloque Crypto'puces 2017 (Rencontres Université-Entreprise): *Effective arithmetic in finite fields based on a parallel Chudnovsky multiplication algorithm*, co-présenté avec K. Atighehchi, Porquerolles, 29 mai- 2 juin 2017.

• Colloque Crypto'puces 2015 (Rencontres Université-Entreprise): *Sur les algorithmes de multiplication dans les corps finis par interpolation sur des courbes algébriques*, Porquerolles, 4-8 mai 2015.

• Liaison Lycée/Université: Journée Rencontre Enseignants du Secondaire/Départements de Mathématiques et d'informatique sur le thème *Sécurité de l'information, aspects mathématiques et informatiques*: *Sécurité de l'Information, Introduction à la cryptologie, "Les Principes"* (45 minutes), vendredi 21 février 2014.

• Journée Codage et Cryptographie , Institut de Mathématiques de Luminy (IML): *Construction de courbes de genre 2 définies sur les rationnels et cryptosystèmes*, 16 mars 2000.

• Conférence au séminaire IC5, Délégation Générale de l'Armement (Paris), 5 octobre 1998: Multiplication dans les corps finis, sous forme de deux exposés:
1) Multiplication dans les corps finis - Généralités
2) Multiplication dans les corps finis par interpolation sur des courbes algébriques.

• Colloque national Journées Algorithmiques, Modèles et Infographie, C.I.R.M (Marseille): *Multiplication rapide dans les corps finis*, 1–5 septembre 1997.

8) Communications sur invitation en école internationale:

• Ecole CIMPA-UNESCO MEXIQUE (Centre International de Mathématiques Pures et Appliquées): Arithmétique, algèbre commutative, géométrie algébrique et applications, en laison avec le calcul formel: Introduction à la géométrie algébrique des courbes - Application en kash (7,5 heures), Aout 2003.

9) Communications en école nationale:

• Ecole Jeunes Chercheurs en Algorithmique et Calcul Formel, Université de Bordeaux 1 (LaBRI) : *Bounds on the bilinear complexity of Multiplication in Any Extension of* $\mathbb{F}_q$, 22–26 mars 1999.

• Deuxième école d'automne AMIcale, C.I.R.M. (Marseille) : *Multiplication rapide dans les corps finis*, 8–12 decembre 1997.

10) Publication dans un bulletin avec audience nationale:

• *On the complexity of multiplication in certain finite extensions of finite fields*, Bulletin numéro 3 de la cellule de Prospective en Cryptographie, Codage et Sécurité des Réseaux de la Délégation Générale de l'Armement, p. 78-89, 29 janvier 1998, Ed. F. Chabaud, J.-M Couveignes.

11) Autres publications:

• *Corps de fonctions algébriques et application à l'étude de la complexité bilinéaire de la multiplication dans les corps finis*, Thèse d'Habilitation à Diriger des Recherches, Université de la Méditerranée, juin 2006.

• *Etude de la construction de courbes de genre 2 et cryptosystèmes*, rapport interne du Centre de l'Armement pour la Sécurité des Systèmes d'Information, Cellule Etudes Cryptographiques, juillet 1999.

• *Etude de la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*, Thèse de Doctorat, Université d'Aix-Marseille II, novembre 1998.

12) Exposés lors de séminaires:

• Journée Crypto CReC (Centre de Recherche des Ecoles de Coëtquidan) - IRISA (Université de Rennes): *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 2 juin, 2022.
• Séminaire GAATI (Géométrie Algébrique et Applications de la Théorie de l'Information), Université de la Polynésie Française à Tahiti: *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 2 mai, 2022.
• Séminaire de l'Institut de Mathématiques de Toulon (IMATH), équipe Informatique et Algèbre appliquée (IAA): *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 7 décembre 2021.
• Séminaire du Laboratoire de Mathématiques pour les Ingénieurs (LMI): *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 24 septembre 2021.
• Séminaire LFANT (Lithe and Fast algorithmic in Number Theory), INRIA Project Team LFANT, CNRS, Institut de Mathématiques de Bordeaux (IMB): *Optimization of the scalar complexity of Chudnovsky^2 multiplication algorithms in finite fields*, 8 juin 2021.
• Séminaire du Master de Mathématiques Fondamentales (spécialité: Géométrie Algébrique et Arithmétique), Centre de Mathématiques et d'Informatique de Chateau-Gombert (CMI), Aix-Marseille Université :*Les codes géométriques de Goppa* , 4 novembre 2019.
• Séminaire de Géométrie Complexe (groupe Analyse, Géométrie et Topologie), Institut de Mathématiques de Marseille (I2M), Aix-Marseille Université :*Familles denses de courbes modulaires, nombres premiers et rang de tenseur symétrique uniforme de la multiplication dans certains corps finis*, 12 Juin 2018.
• Séminaire GAATI (Géométrie Algébrique et Applications de la Théorie de l'Information), Université de la Polynésie Française à Tahiti: *Tours ordinaires de corps de fonctions et rang de tenseur de la multiplication dans les extensions de $\mathbb{F}_2$ et $\mathbb{F}_3$*, 13 Avril 2017.
• Séminaire INFRES, Département Informatique et Réseaux (INFRES), Laboratoire Communications et Traitement de l'Information (LCTI), Groupe Mathématiques de l'Information, des Communications et du Calcul (MIC2), Telecom ParisTech, Paris: *Tours ordinaires de*

corps de fonctions et rang de tenseur de la multiplication dans les extensions de $\mathbb{F}_2$ *et* $\mathbb{F}_3$, 7 juillet 2015.
• Séminaire de Mathématiques, Université de Besançon: *Familles de courbes définies sur tout corps fini avec un nombre de classes asymptotiquement grand*, 5 mai 2010.
• Séminaire GAATI (Géométrie Algébrique et Applications de la Théorie de l'Information), Université de la Polynésie Française à Tahiti: *Courbes définies sur un corps fini quelconque ayant un nombre de classes dépassant les bornes de Lachaud - Martin-Deschamps*, 1er Avril 2010.
• Séminaire de Cryptographie (IRMAR-CELAR), Université Rennes I- DGA: *Courbes définies sur un corps fini quelconque ayant un nombre de classes dépassant les bornes de Lachaud - Martin-Deschamps*, 19 juin 2009.
• Séminaire d'Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR), Université de la Méditerranée (Marseille): *Existence des diviseurs de dimension nulle (en particulier non-spéciaux de degré* $g-1$*) dans les corps de fonctions algébriques définis sur* $\mathbb{F}_q$, 22 janvier 2009.
• Séminaire d'Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR), Université de la Méditerranée (Marseille): *Corps de fonctions algébriques et application à l'étude de la complexité bilinéaire de la multiplication dans les corps finis (Soutenance HDR)*, 26 juin 2006.
• Séminaire d'Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR), Université de la Méditerranée (Marseille): *Descente du corps de définition d'une tour de corps de fonctions et applications*, 13 janvier 2005.
• Séminaire de Cryptographie (IRMAR-CELAR), Université Rennes I- DGA: Complexité bilinéaire de la multiplication dans les corps finis et corps de fonctions algébriques, 12 décembre 2003.
• Séminaire du Groupe de Recherche en Informatique et Mathématiques (GRIMM), Université Toulouse II : *Complexité bilinéaire de la multiplication dans les corps finis et corps de fonctions algébriques*, 12 décembre 2002.
• Séminaire du Groupe de Recherche en Informatique et Mathématiques (GRIM), Université de Toulon, *Construction effective d'algorithmes de multiplication rapide*, 3 décembre 2002.
• Séminaire de Mathématiques (Groupe de travail), Université de la Polynésie Française à Tahiti: *Théorie des codes correcteurs d'erreurs* (4h, novembre 2001).
• Séminaire de Mathématiques, Université de la Polynésie Française à Tahiti: *Construction d'une tour de corps de Fonctions algèbriques*, 5 mai 2001.
• Séminaire d'Algèbre et Applications, Université des Antilles-Guyane à Pointe-à-Pitre (Guadeloupe): *Construction de courbes de genre 2 définies sur les rationnels - Application à la construction de cryptosystèmes*, Juin 2000.
• Séminaire de Cryptographie du Centre de l'Armement pour la Sécurité des Systèmes d'Information, Centre d'Electronique de l'Armement: *Construction de courbes de genre 2 définies sur les rationnels - Application à la construction de cryptosystèmes (Partie 2)*, 21 juillet 1999.
• Séminaire de Cryptographie du Centre de l'Armement pour la Sécurité des Systèmes d'Information, Centre d'Electronique de l'Armement: *Construction de courbes de genre 2 définies sur les rationnels - Application à la construction de cryptosystèmes (Partie 1)*, 20 juillet 1999.
• Séminaire de Calcul Formel et Complexité de l'Institut de Recherche en Mathématiques de Rennes (IRMAR), Université de Rennes I: *Etude de la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*, 2 juin 1999.
• Séminaire d'Algorithmique du Laboratoire d'Informatique et Algorithmique - Fondements et Applications, Université de Paris VII, Jussieu: *Etude de la complexité bilinéaire de la*

multiplication dans les corps finis par interpolation sur des courbes algébriques, 25 mai 1999 (programmé).
• Séminaire de Théorie des Nombres, Université de Caen: *Etude de la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*, 20 mai 1999 (programmé).
• Séminaire de Mathématiques du Centre de Recherche des Ecoles de Coetquidan, ESM St Cyr: *Deux applications des courbes algébriques - la multiplication dans les corps finis et crypto-systèmes basés sur le logarithme discret*, 22 avril 1999.
• Séminaire de l'Ecole Supérieure des Sciences de l'Informatique, Sophia-Antipolis: *Etude de la complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques*, 3 décembre 1998.
• Séminaire d'Algèbre de Marseille, Université d'Aix - Marseille I et II: *Bornes de la complexité de la multiplication dans toutes les extensions de* $\mathbb{F}_q$, 6 octobre 1998.
• Séminaire d'Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UPR 9016), Université de la Méditerranée (Marseille): *Complexité de la multiplication dans les extensions de* $\mathbb{F}_{q^r}$, 18 juin 1998.
• Séminaire du Groupe d'Etude du Codage de Toulon, Université de La Garde : *Complexité de la multiplication et courbes avec beaucoup de points dans les corps finis*, 9 juin 1998.
• Séminaire Algorithmique et Cryptographie au Laboratoire d'Informatique de Toulon, Université de La Garde : *Multiplication rapide dans les corps finis*, mars 1998.
• Séminaire Théorie des Nombres et Algorithmique au Centre de Mathématiques et d'Informatique de Marseille à Château Gombert, Université de Provence: *Multiplication rapide dans les corps finis*, octobre 1997.
• Séminaire du Groupe d'Etude du Codage de Toulon, Université de La Garde: *Complexité de la multiplication dans certains corps finis par les courbes maximales*, mai 1997.
• Séminaire d'Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UPR 9016), Université de la Méditerranée (Marseille): *Complexité de la multiplication dans certains corps finis par les courbes Hermitiennes*, Mai 1997.

12) Encadrement doctoral

a) Thèses de doctorat

• Direction de la Thèse de Doctorat de Mahdi Koutchoukali (en cours depuis septembre 2022), co-encadré avec Julia Pieltant (MCF CNAM): *Sur l'existence des diviseurs non-spéciaux de degré g-1 dans les corps de fonctions algébriques définis sur un corps fini.*

• Co-direction (avec A. Bonnecaze) de la Thèse de Doctorat de Bastien Pacifico de septembre 2018 au 15 décembre 2022 (date de soutenance) : *Sur les stratégies de construction des algorithmes de type Chudnovsky pour la multiplication dans les corps finis et leur complexité bilinéaire associée.*

• Co-direction (avec A. Bonnecaze) de la Thèse de Doctorat de Thanh-Hung Dang (bourse du Viet-Nam) de mars 2016 au 25 mai 2020 : *Complexité scalaire des algorithmes de type Chudnovsky de multiplication dans les corps finis.*

• Co-direction (avec A. Bonnecaze) de la Thèse de Doctorat de Mila Tukumuli (actuellement Gérant d'une entreprise en Nouvelle-Calédonie) de septembre 2009 au 13 septembre 2013 (date de soutenance): *Etude de la construction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis.*

• Direction de la Thèse de Doctorat de Julia Pieltant (actuellement MCF du CNAM de Paris)) de septembre 2009 au 12 décembre 2012 (date de soutenance): *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis.*

• Encadrement (90%) de la Thèse de Doctorat de Jean Chaumine (MCF HC de l'Université de la Polynésie Française, actuellement Directeur de l'ESPE de l'UPF) de septembre 2002 au 28 avril 2005 (date de soutenance): *Corps de fonctions algébriques et algorithme de D.V. et G.V. Chudnovsky pour la multiplication dans les corps finis.*

b) Mémoires de Master 2

• Encadrement du mémoire de Master 2 (Recherche) Mathématiques Fondamentale Géométrie algébrique et arithmétique (Aix-Marseille Université, MF 2019-2020) de l'étudiante Yousra Kasbani: *Sur la descente du corps de définition des corps de fonctions algébriques définis sur les corps finis.*
• Encadrement du mémoire de Master 2 (Recherche) Mathématiques Discrétes et Fondement de l'Informatique (Aix-Marseille Université, MDFI 2017-2018) de l'étudiant Bastien Pacifico (classé 1er du M2): *Sur les stratégies de construction des algorithmes de type Chudnovsky pour la multiplication dans les corps finis.*
• Encadrement du mémoire de Master 2 (Recherche) Mathématiques Discrétes et Fondement de l'Informatique (Aix-Marseille Université, MDFI 2016-2017) de l'étudiant Mahdi Koutchoukali: *Sur l'existence des diviseurs non-spéciaux de degré $g-1$ dans les corps de fonctions algébriques définis sur un corps fini.*
• Encadrement du stage de 3ème année (durée: 4 mois) de l'Ecole Polytechnique (Palaiseau) de l'étudiant François Bonnal (spécialité de 3ème année: Informatique/Réseaux et Sécurité): *Amélioration des algorithmes de multiplication de type Chudnovsky* (recherche, à l'aide de simulation en Magma, de représentations adaptées des espaces de Riemann-Roch afin de minimiser la complexité scalaire), mars-juillet 2016.
• Encadrement du mémoire de Master 2 Recherche Mathématiques Fondamentales (Univ. de Provence, 2010-2011) de l'étudiant Michaël Beliardo : *Les fonctions Zetas d'une tour optimale de corps de fonctions algébriques définis sur* $\mathbb{F}_4$.
• Encadrement du mémoire de Master 2 Recherche Sécurité de l'Information parcours Mathématiques, Cryptologie, Codages et Applications(Univ. de Limoges, SI 2008-2009) de l'étudiante Julia Pieltant (classée 1ère du M2): *Autour de la multiplication dans les corps finis.*
• Encadrement du mémoire de Master 2 (Recherche) Mathématiques Discrétes et Fondement de l'Informatique (Univ. de la Méditerranée, MDFI 2008-2009) de l'étudiant Mila Tukumuli: *Galois Counter Mode: un chiffrement par bloc avec authentification.*
• Encadrement du mémoire de Master 2 (Professionnel) Mathématiques et Informatique des Nouvelles Technologies (Univ. de la Méditerranée, MINT 2008-2009) des étudiants G. Bardet et S. Narbo: *Courbes elliptiques et application à la cryptographie.*

13) Jurys de thèse (comme rapporteur ou examinateur)

• Membre (rapporteur) de la Thèse de Doctorat de Édouard Rousseau, co-dirigée par Luca Del Feo, Hugues Randriambolona, et Éric Schost, le 12 juillet 2021 : *Efficient Arithmetic of finite field extensions.*

• Membre (co-directeur et examinateur) de la Thèse de Doctorat de Thanh-Hung Dang, le 25 mai 2020 : *Complexité scalaire des algorithmes de type Chudnovsky de multiplication dans les corps finis.*

• Membre du jury (examinateur) de la Thèse de Doctorat de Stéphanie Dib dirigée par le Directeur de Recherche (CNRS) François Rodier, le 11 décembre 2013 à l'Université d'Aix-Marseille: *Distribution de la non-linéarité des fonctions booléennes.*

• Membre du jury (co-directeur et examinateur) de la Thèse de Doctorat de Mila Tukumuli, le 13 septembre 2013 à l'Université d'Aix-Marseille: *Etude de la construction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis.*

• Membre du jury (directeur et examinateur) de la Thèse de Doctorat de Julia Pieltant, le 12 décembre 2012 à l'Université d'Aix-Marseille: *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis.*

• Membre du jury (examinateur) de la Thèse de Doctorat (PhD) de Seher Tutdere dirigée par le Professeur Henning Stichtenoth, le 30 mai 2012 à Sabanci University à Istambul (Turquie): *On the asymptotic theory of function fields over finite fields.*

• Membre du jury (examinateur) de la Thèse de Doctorat de J. Chaumine, le 28 avril 2005 à l'Université de la Polynésie Française: *Corps de fonctions algébriques et algorithme de D.V. et G.V. Chudnovsky pour la multiplication dans les corps finis.*

14) Diffusion de la recherche: activités de referee et de reviewer

a) Referee :

Depuis 2000, pour les revues internationales:

• Acta Arithmetica
• Journal of Symbolic Computation (Elsevier)
• Theoretical Computer Science (Elsevier) (pour la conférence CAI 2018)
• Journal of Algebra and its Applications (World Scientific)
• Discrete Mathematics (Elsevier)
• J. of Pure and Applied Algebra (Elsevier)
• Mathematics of Computation (AMS)
• J. of Complexity (Elsevier)
• IEEE Transactions on Information Theory
• J. of Computational and Applied Mathematics (Elsevier)
• Finite Fields and Their Applications (Elsevier)
• Advances in Mathematics of Communications (AIMS) (Editeur invité en 2014 pour la conférence Geocrypt 2013)
• Linear and Multilinear Algebra
• Lecture Notes in Computer Science (Springer)
• Journal of Algebra

b) Reviewer :

En 2005-2006, pour la Division Mathematical Reviews de l'American Mathematical Society.

15) Diffusion de la recherche: organisation de colloques ou journées thématiques

a) Comités de pilotage (Steering Committee)

• Membre nommé du Comité de Pilotage des colloques internationaux AGC^2T "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, depuis novembre 2019.

• Membre nommé du Comité de Pilotage du Forum AMUSEC (Forum de Cybersécurité de l'Université d'Aix-Marseille) depuis novembre 2016.

b) Comités scientifiques (ou de programme)

• Membre du Comité Scientifique du colloque international COnference on alGebraic varieties over fiNite fields and Algebraic geometry Codes (COGNAC-2023) prévu du 13/02/2023 au 17/02/2023, co-responsable de la constitution du dossier de candidature pour le CIRM (soumission acceptée, cf. Section suivante pour détails complémentaires).

• Membre du Comité Scientifique du colloque international AGC^2T17 "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, 10-14 juin 2019.

• Membre nommé du Comité Scientifique du colloque international Conference on Algebraic Informatics (CAI 2017), Kalamata, Grèce, 25-28 juin 2017. Co-chair du track 2: Cryptography and Coding Theory.

• Membre du Comité Scientifique du colloque international Conference on Geometry and Cryptography (Geocrypt), Tahiti, octobre 2013.

• Membre du Comité Scientifique du colloque international AGC^2T14 "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, juin 2013.

• Membre nommé du Comité Scientifique du colloque international Conference on Algebraic Informatics (CAI 2013), Porqueroles (France), septembre 2013.

• Membre nommé du Comité Scientifique du colloque International Workshop on the Arithmetic of Finite Fields (Waifi 2012), Bochum (Allemagne), juillet 2012.

• Membre nommé du Comité Scientifique du colloque international Conference on Geometry and Cryptography (Geocrypt), Guadeloupe, avril 2009.

• Membre du Comité Scientifique du colloque international S.A.G.A Symposium of Algebraic Geometry and Applications: Coding Theory and Cryptography, en l'honneur du 60ième anniversaire de Gilles Lachaud, Tahiti, mai 2007.

c) Comités d'organisation

• Co-organisateur du **Mois thématique** *Arithmetic and Information Theory* **(février 2023)**, organisé au CIRM par l'équipe Arithmétique et Théorie de l'Information ATI (CNRS/AMU)), et adossé au Premier Semestre de la Chaire Morlet portée par un membre de l'équipe ATI (Samuele Anni). Plus particulièrement, j'ai été en charge avec Yves Aubry de la constitution du dossier de candidature de la Conférence internationale : COnference on alGebraic varieties over fiNite fields and Algebraic geometry Codes (COGNAC-2023) et co-organise cette future conférence prévue du 13/02/2023 au 17/02/2023.

• Membre du Comité d'organisation (General Chair) du colloque international AGC^2T17 "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, responsable de la constitution du dossier de candidature pour le CIRM, 10-14 juin 2019.

• Membre du Comité d'organisation de la première édition des Journées sécurité AMUSEC, Rencontre annuelle des acteurs de la sécurité des systèmes d'information de la région PACA, à Polytech Marseille, Luminy, le 24 mars 2016.

• Membre du Comité d'organisation (Co-chair) du colloque international AGC^2T14 "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, juin 2013.

• Membre du Comité d'organisation du colloque international S.A.G.A Symposium of Algebraic Geometry and Applications: Coding Theory and Cryptography, en l'honneur du 60ième anniversaire de Gilles Lachaud, Tahiti, mai 2007.

Projets et collaborations

1) Groupes de recherche

• Membre du groupe de recherche:

GDR IM Informatique Mathématique sous-groupe C2: codage et cryptographie

• Responsable du pôle Luminy pour GDR IM/ GT-C2.

• Coordonnateur de l'équipe de mathématiques de Polynésie Française au sein du GDR IM, 2004-2008.

2) Projets nationaux et internationaux (public et industriel)

• Membre d'une équipe du Projet National:

ACI Cryptographie (Action Concertée Incitative 2000-2002 et 2002-2004) dirigée par G. Lachaud et R. Rolland.

Membres: Aubry, Ballet, Barthélemy, Cherdieu, Driencourt, Lachaud, Rolland, Tsfasman, Vladut.

Thèmes: Générateurs et distributeurs de clefs, groupes algébriques à logarithme discret robustes, codes d'authentification, confidentialité des transmissions, fonctions courbes.

3) Missions de recherche: invitations

a) Missions nationales:

• **Dans Équipe en Émergence Sécurité-Défense EPN 15 "Stratégies" - Chaire de Criminologie)** du Conservatoire National des Arts et Métiers, Paris: janvier 2020 (1 semaine).

• **Dans le Groupe Mathématiques de l'Information, des Communications et du Calcul (MIC2)** du Laboratoire Communications et Traitement de l'Information (LCTI) au sein du Département Informatique et Réseaux (INFRES), Telecom ParisTech, Paris: novembre 2018 (1 semaine), Convention de séjour sabbatique du 15 juin au 10 juillet 2015 (1 mois).

• **Au Laboratoire de l'Ecole Polytechnique (LIX), équipe INRIA/Crypto** dirigée par Daniel Augot (DR INRIA), octobre 2013 (1 semaine).

• **A l'UPF, Laboratoire GAATI en Polynésie Française**: Avril-mai 2022 (2 semaines), Avril 2017 (2 semaines), Avril 2016 (2 semaines) , Novembre 2012 (1 mois), Avril 2010 (2 semaines).

• **A l'Institut de Mathématiques de Luminy (CNRS UPR 9016) à Marseille**, équipe Arithmétique et Théorie de l'Information: juin 2006 (2 semaines), janvier 2005 (4 semaines), juin-juillet 2004 (3 semaines), novembre-décembre 2003 (6 semaines), novembre-décembre 2002 (5 semaines), décembre 2001 (3 semaines), décembre 2000 (1 semaine), mars 2000 (3 semaines), décembre 1999 (1 semaine), novembre 1999 (1 semaine avec participation au colloque international AGCT 7 au CIRM).

• **Au Département d'Analyse Algébrique de Jussieu à Paris** (Paris VI) en collaboration avec Dominique Lebrigand: mars et mai 2004 (1 semaine), janvier 2000 (1 semaine), décembre 1999 (2 jours).

b) Missions internationales:

• **A l'Université Indépendante de Moscou, Unité Mixte Internationale Poncelet**, à Moscou (Russie): invitation par le professeur Michaël Tsfasman, septembre 2013 et juin 2014 (une semaine, pour le semestre thématique Global Field et une semaine prévue pour le colloque Algebraic Geometry and Number Theory à l'occasion du 60ème anniversaire de Michael A. Tsfasman and Sergei G. Vladut).

• **A Macquarie University, Division of Information and Communication Sciences, Department of Computing, Centre for Advanced Computing-Algorithms and Cryptography (ACAC)**, à Sydney (Australie): invitation par le Professeur I. Shparlinsky (Membre de l'Australian Academy of Sciences), décembre 2006 (2 semaines).

Activités Administratives

Voici une description de la participation à la vie de l'établissement et de la communauté relative à ma discipline, au travers différentes activités administratives d'ordre général ou spécifique à l'enseignement ou à la recherche.

1) **Général :**

Echelon national :

• **Membre invité du Conseil d'Administration du Centre Internationale de Rencontres Mathématiques (CIRM)**, en tant que Vice-président de la SMF en charge de la Cellule de diffusion, depuis novembre 2020.

Dans ce cadre de mes activités liées au CIRM:

- j'ai représenté la SMF lors de l'évaluation du CIRM du 12 juillet 2022 (organisation de la visite guidée de la Cellule de diffusion de la SMF pour les membres du Jury, entretien d'une heure avec le Jury d'évaluation).

-j'ai représenté la SMF lors de la cérémonie d'hommage pour le départ de à la retraite de Patrick Foulon: élocution dub discours de remerciement au nom de la SMF.

• **Membre nommé du Bureau de la SMF**, Vice-président en charge de la Cellule de Diffusion de la SMF ((site de Luminy, 26 juin 2020-2023). Dans le cadre de cette fonction:

- co-porteur du projet (avec Fabien Durand, Président de la SMF) de mise en place des abonnements gratuits à toutes les revues de la SMF pour des universités africaines (une trentaine pour l'instant) pour une période de 5 ans ainsi que pour les pays ayant peu de moyens (Action pour la Science ouverte).

- co-instigateur d'opérations de dons de livres organisée par la Cellule (stockage, conditionnement, et expédition de livres publiés par la SMF et de livres d'enseignement des mathématiques donnés par des particuliers) dans le cadre des désherbages physique de novembre 2020 et ceux administratifs annuels depuis 2022: en faveur de l'APSA (Association pour la Promotion Scientifique de l'Afrique) et du Burkina Faso (cette dernière action en collaboration avec le service des Relations Internationales d'AMU en 2020, en faveur de
.

• **Membre élu du Conseil d'administration de la Société Mathématique de France (SMF)** (12 juin 2020-2023).

• **Membre extérieur du Comité de sélection** pour le poste de MCF en Mathématiques de l'UPF, (co-responsable de l'organisation de la visioconférence sur le campus de Luminy), année 2013.

• **Membre extérieur du Comité de sélection** pour le poste de MCF en Informatique (cryptographie) de l'Université Sud Toulon Var, année 2010.

• **Membre extérieur du Comité de sélection** pour les postes de MCF en Mathématiques de l'UPF (responsable de l'organisation de la visioconférence sur le campus de Luminy), année 2009.

• **Membre élu au Conseil National des Universités (CNU section 25, collège B)**, années 2003-2007 et années 2008-2011.

• **Membre du jury du CAPES Externe de Français-Tahitien (option Mathématiques)**, correction de l'épreuve écrite 2006, années 2005-2006.

<u>Echelon local :</u>

• **Membre élu au Conseil de l'UFR Sciences d'AMU**: tête de la liste Cap sur la Confiance (Collège B), depuis le 10 novembre 2021.

• **Rapporteur interne nommé par le Conseil Scientifique d'AMU** pour expertise de dossiers (CRCT etc...), année 2018.

• **Membre du Groupe de Travail "formation du comité de sélection du poste MCF 25 profil Mathématiques Discrètes et Interactions avec l'Informatique, année 2018"**, février 2018, publication au fil de l'eau (comité prévu en octobre 2018).

• **Membre interne nommé du comité de sélection** pour le poste MCF 25 (profil: Géométrie, Dynamique, Topologie) de l'AMU, année 2018.

• **Membre de la commission des bureaux (site de Luminy)**, de 2016 à 2017.

• **Membre interne nommé du Comité de sélection** (en tant que représentant de la gouvernance et de la composante) pour le poste de MCF en Mathématiques (profil: Théorie des nombres et géométrie arithmétique) de l'AMU, année 2015.

• **Membre interne nommé du Comité de sélection** pour le poste de MCF en Mathématiques (profil: Mathématiques discrètes: logique, théorie des nombres et théorie de l'information) de l'AMU, année 2014.

• **Membre élu du Conseil de Département de Mathématiques** de l'AMU, 2012-2016.

• **Membre titulaire du Conseil Scientifique** de l'UPF, années 2004-2007.

• **Membre titulaire (assesseur) de la commission de spécialistes (section 25 et 27)** de l'UPF, années 2004-2007.

• Président de Jury des bachalauréats généraux et technologiques de Polynésie Française, année 2004-2005.

• Président de Jury du bachalauréat technologique de l'Académie d'Aix-Marseille, année 2017-2018.

2) <u>Recherche :</u>

• **Membre nommé** par la Commission Recherche du Conseil Académique d'AMU (CAcR) **dans un comité** *Ad hoc* **volet recherche** afin d'évaluer l'Activité de recherche des enseignants-chercheurs candidats à l'avancement local, pour l'année 2022.

• **Membre nommé dans le Comité scientifique de l'UFR Sciences**, depuis le 1er décembre 2021, chaque année: expertise des dossiers de candidature dans le cadre des appels à projets Recherche de la REGION SUD (AAP, volet exploratoire), expertise des dossiers de demande de "Congés pour Recherches ou Conversions thématiques" (CRCT) au titre de l'établissement (pour l'année universitaire 2022-23), expertise des dossiers FIR Accueil d'enseignants-chercheurs invités 2023.

• **Membre suppléant** (suppléant d'Alexis Bonnecaze) **du Bureau de la Direction de l'I2M**, en cours (depuis le 1er Mars 2018).

• **Responsable adjoint** du Groupe de recherche Algèbre, Géométrie, Logique et Représentations (AGLR), groupe de l'I2M comportant trois équipes de recherche: équipes Arithmétique et Théorie de l'Information (ATI), Logique de la Programmation (LDP), et Représentation des Groupes Réductifs (RGR), en cours (depuis le 1er Mars 2018).

• **Responsable** de l'équipe Arithmétique et Théorie de l'Information, en cours (depuis le 1er Mars 2018).

• **Membre de Comités de Suivi de Thèses**:

- au sein de l'Ecole Doctorale de Mathématiques et d'Informatique (ED184) de l'AMU, 2017-2022: Leonardo Colo (sur proposition du Directeur de Thèse David Kohel).

- Au sein de l'Ecole Doctorale de l'Université de Toulon et du Var, 2019-2022: Ali Issa (sur proposition des Directeurs de thèse Yves Aubry et Fabien Herbaut).

• Participation à l'élaboration du Comité de sélection pour le poste MCF 25/26 de l'IUT (AMU) sur demande du responsable de l'équipe ATI, décembre 2016.

• Rédaction de la partie Recherche de la fiche du poste MCF 25/26 de l'IUT (AMU) sur demande du responsable de l'équipe ATI, juin 2016.

• Rédaction avec Alexis Bonnecaze (resp. de l'équipe ATI) du Rapport d'activité de l'équipe d'ATI pour le plan quadriénnal 2012-2015, avril 2016.

• **Membre nommé du Comité de Suivi de Thèses** au sein de l'Ecole Doctorale de Mathématiques et d'Informatique (ED184) de l'AMU, année 2014: chargé (sous la direction de S. Troubetzkoi) de l'organisation des entretiens des doctorants en Mathématiques en 4ème et 5ème année du site de Luminy.

• **Directeur du laboratoire GAATI** en 2007 puis démission en janvier 2008 pour cause de mutation. Responsable de la constitution du dossier pour le plan quadriénnal 2008-2011: avis favorable au renouvellement de l'équipe (MSTP, AERES) pour une durée de 4 ans.

• **Co-fondateur de la première Unité de Recherche en Mathématiques** (démarches administratives relatives, constitution du dossier scientifique), reconnue par le Ministère, **de l'Université de la Polynésie Française** : Equipe d'Accueil Géométrie Algébrique et Applications à la Théorie de l'Information, plan quadriénnal 2004-2007.

3) **Enseignement :**

• **Co-responsable de la transformation de l'initiative du tutorat de mathématiques en Cordée de la réussite en partenariat avec le Rectorat (co-gestion du dispositif en tant que tête de cordée portée par la Faculté des Sciences d'AMU)** sur la demande de Laurence Mouret (Doyenne de la Faculté des sciences d'AMU), d'Anne Ribaud (VP AMU déléguée à l'orientation et à l'insertion professionnelle en charge de l'égalité des chances - chargée de mission projet Ascenseur social), et de Nora Abid (chargée de mission Egalité des chances d'AMU). Projet en cours (avril-mai 2023).

• **Co-organisation de la Master Class**(avec D. Kohel et X. Roulleau): Cryptographie et Codage correcteur d'erreurs à base de courbes algébriques et surfaces, Luminy, 10-19 avril 2019.

• **10ème Salon des Masters, AMU**: tenue du stand (avec Xavier Roulleau) de Mathématiques Fondamentales, 02/02/2019.

• **Membre de l'équipe pédagogique** avec Julien Keller, David Kohel, Marc-Hubert Nicole, Xavier Roulleau, Erwan Rousseau, pour la constitution du programme de Master 2 Recherche de Mathématiques Fondamentales, thématique: Géométrie Algébrique et Arithmétique, Année 2019-2020.

• **Membre nommé de Jury de L2** Mathématiques Générales à AMU depuis 2018.

• **Membre d'un Groupe de Travail pour la Licence** Miash (préparation de la maquette 2018): Groupe de travail pour le module Fondements mathématiques et Analyse, octobre-novembre 2017.

• **Responsable d'un Groupe de Travail pour la Licence** de Mathématiques (Math Géné et Math Info) (préparation de la maquette 2018): Groupe de travail pour le module Histoire et Philosophie des Mathématiques, octobre-novembre 2017.

• **Responsable pédagogique** du Master 1 de Mathématiques et Applications à l'Université de la Méditerranée, année 2010-2011 et 2011-2012.

• Membre des commissions pédagogiques de validation des acquis (Mentions Sciences physiques, Mathématiques et Informatique), à l'Université de la Polynésie Française, années 2005-2006.

• Membre de Jurys des diplomes de DEUG MIAS, SM et Licence de Mathématiques délivrés par l'Université de la Polynésie Française de 2001 à 2008.

• **Responsable pédagogique** des DEUG MIAS à l'Université de la Polynésie Française, années 2001-2002 et 2002-2003.

• Tuteur du stage informatique de fin d'études cycle ingénieur àl'Ecole Centrale de Lille, d'un étudiant de 3ème année de ESM St Cyr, année 1999-2000.

4) **Autres activités :**

• Deuxième Journée consacrée aux Lycées au CIRM (les journées de diffusion du CIRM), tenue du stand de la SMF à destination des personnels enseignants et de l'Inspection académique (dans le cadre de la liaison Lycée/enseignement supérieur), échanges sur les réformes de l'enseignement et la place des maths, le rôle de la SMF, dons de goodies pour sensibiliser les personnels à soutenir la SMF (tutelle du CIRM), jeudi 13 octobre 2022.

• *Ambassadeur pour la Rencontre Déclic numéro 217(Dialogues Entre Chercheurs et Lycéens pour les Intéresser à la Construction des Savoirs) de médiation scientifique*: thème de recherche: Géométrie algébrique appliquée à la théorie de l'information, au Lycée Marseilleveyre, mardi 16 novembre 2021.

• *Présentation des Métiers de la Recherche* au Lycée Cours Bastide, à Marseille, jeudi 26 janvier 2017.

• *Carrefour des Métiers* au Collège Jean de la Fontaine de Gémenos: tenue du stand Recherche (présentation à plusieurs groupes d'élèves de 3ème), jeudi 10 mars 2016.

• Vice-président et co-fondateur de l'Association des Mathématiciens en Polynésie (A.M.P.) de 2006 à 2008.

• Membre du jury à l'entretien de motivation au concours d'entrée à l'Ecole Internationale des Sciences du Traitement de l'Information en juillet 1995.