Rapport d'Activités Quadriennal du Laboratoire de Mathématiques

Période 2008-2011

1 Nom du Laboratoire

Géométrie Algébrique et Applications à la Théorie de l'Information (**EA 3893 GAATI**).

2 Constitution de l'équipe

L'équipe du Laboratoire de **Géométrie Algébrique et Applications à la Théorie de l'Information** de l'Université de la Polynésie française est constituée de :

- **Jean-Marie Goursaud**, Professeur, Directeur du Laboratoire.
- **David Adam**, Maître de Conférences.
- **Gérald Bourgeois**, Maître de Conférences.
- **Jean Chaumine**, Maître de Conférences.
- **Eric Férard**, Maître de Conférences.
- **Roger Oyono**, Maître de Conférences.

Les anciens membres du Laboratoire GAATI sont :

- **Stéphane Ballet** jusqu'en 2008.
- **Régis Blache** jusqu'en 2007.

3 Bilan, objectifs et travaux

3.1 Bilan et objectifs

Le laboratoire GAATI est le premier laboratoire de mathématiques crée en 2004 à l'Université de la Polynésie française. Il est l'aboutissement d'une dynamique de recherche universitaire en mathématiques qui s'est développée depuis quelques années suite à l'arrivée de jeunes enseignants-chercheurs spécialisés en mathématiques et ses applications à la théorie de l'information. Sa mise en place traduit notre volonté de maintenir un niveau d'enseignement supérieur de qualité. Il nous permettra aussi d'encadrer de jeunes Polynésiens afin de former de futurs enseignants-chercheurs susceptibles d'exercer dans cette université.

Le domaine de recherche de notre équipe porte sur la géométrie algébrique et ses applications à la théorie de l'information : cryptographie, codage correcteurs d'erreurs, algorithmique. Ce domaine récent et innovant est très prometteur et capable d'apporter de nouvelles perspectives. Il représente un réel potentiel dans le domaine des nouvelles technologies dont l'importance dans la société moderne n'est plus à démontrer.

3.1.1 Bilan de la période 2008-2011

Le laboratoire GAATI s'était fixé des objectifs précis pour cette période, à savoir, obtenir des résultats de niveau international dans le domaine de la recherche (la qualité et le volume des publications sont très satisfaisants). Le laboratoire totalise 19 publications de rang A ainsi que 5 publications dans des colloques internationaux avec comité de lecture. Plusieurs projets de coopération et de partenariat sont en cours. Des relations privilégiées avec l'université de Marseille-Luminy et son institut de recherche en mathématiques (IML) reconnu internationalement, ont permis un réel développement de nos recherches et en particulier l'organisation conjointe du colloque international SAGA 2007 à Tahiti regroupant une cinquantaine de chercheurs en mai 2007. Suite au départ de deux des membres du Laboratoire en 2007 et 2008 leur renouvellement a néanmoins permis la poursuite des objectifs fixés lors de l'élaboration du plan.

D'autre part nous avons demandé à plusieurs reprises l'octroi d'un local adapté aux besoins du laboratoire, ce local devant faire office de bibliothèque de recherche et permettre l'accueil correct de chercheurs extérieurs. Cette demande faisait partie des recommandations faites par l'AERES lors de son évaluation de 2008.

Un local nous a effectivement été attribué en Septembre 2009. Toutefois sa situation géographique excentrée ne le rend pas fonctionnel.

De plus, le budget du laboratoire GAATI (5000€ pour 5 enseignants-chercheurs à temps plein) compte tenu de l'isolement géographique, ne permet pas à ses membres de participer correctement à l'activité internationale mathématique aussi bien en termes de participation régulière à des colloques qu'en terme d'achats de revues ou de livres mathématiques. Pour réaliser ces objectifs validés par l'AERES (au moins une mission par enseignant-chercheur actif et par an), l'estimation faite lors de la précédente évaluation était de 3000€ par enseignant-chercheur.

Enfin on pourra constater que les membres du laboratoire doivent assurer une charge importante d'enseignement, nettement supérieure aux 192h statutaires. De plus, certains d'entre eux doivent exercer des responsabilités administratives et pédagogiques comptabilisées d'ailleurs en heures supplémentaires.

3.1.2 Objectifs du plan 2012-2015

Le premier colloque international SAGA organisé par notre équipe, conjointement avec l'IML, en mai 2007 à Tahiti a eu un retentissement international. Nous avons prévu qu'une seconde édition de cet évènement se tienne durant ce plan quadriennal.

Par ailleurs, des discussions sont en cours autour d'un projet fédérant des chercheurs du Pacifique sud (notamment de Nouvelle-Zélande, du Chili et de l'Australie). Cette association est centrée sur les aspects mathématiques de la cryptographie dans le cadre du futur programme Southern PAcific Mathematical CRYPTOgraphy community (SPAMCRYPTO). Ce dernier a l'ambition de promouvoir des collaborations et la tenue de conférences dans la région Pacifique. Des rencontres informelles en ce sens ont déjà été amorcées entre membres de notre laboratoire et ceux du département de Mathématiques de l'Université de Bio-Bio (Concepcion, Chili). Enfin, des contacts prometteurs ont été pris avec des membres du département de Mathématiques de l'Université d'Auckland.

Des collaborations avec des chercheurs d'universités japonaises sont envisagées en vue de codiriger des thèses d'étudiants nippons.

Rappelons une fois de plus qu'afin de travailler dans des conditions décentes, nous souhaitons que notre laboratoire dispose d'un local spécifique. Le laboratoire pourra ainsi atteindre un niveau de fonctionnement normal et pourra se déployer et se développer de manière saine et sereine.

3.2 Thèmes et travaux de recherche

Le domaine de recherche de notre équipe concerne la géométrie algébrique et l'arithmétique des courbes ainsi que leurs applications en théorie de l'information (codages correcteurs d'erreurs, cryptographie).

Nos travaux ont pour objet la géométrie algébrique (théorique et effective) des courbes sur les corps finis. Plus précisément, les thèmes de recherche étudiés portent sur les sujets suivants :

1. Complexité bilinéaire de la multiplication dans les corps finis par interpolation sur des courbes algébriques. Construction effective d'algorithmes de multiplication.

2. Sommes exponentielles et courbes d'Artin-Schreier.

3. Courbes algébriques de petit genre et leurs applications en cryptographie. Calcul du nombre de points et algorithmes d'addition dans les jacobiennes sur les corps finis. Problème inverse du comptage de points. Etude des pairings sur les courbes elliptiques et hyperelliptiques. Ces objets géométriques jouent un rôle de plus en plus important dans la construction de cryptosystèmes.

4. Courbes modulaires et opérateurs de Hecke. Détermination complète des courbes modulaires nouvelles de genre 3. Approche de la conjecture sur le nombre fini de courbes modulaires (non-nouvelles) de genres 2 et 3.

5. Polynômes à valeurs entières : étude des factorielles généralisées de Bhargava. Applications aux théorèmes de type Pólya sur les fonctions entières en caractéristique positive.

6. Tours de corps de fonctions algébriques définis sur des corps finis. Construction de tours de corps de fonctions minorant la borne de Vlăduţ-Tsfasman-Xing (Modules de Drinfeld).

7. Fonctions APN et fonctions de petite uniformité différentielle.

8. Systèmes à clé publique en cryptographie (en particulier le système NTRU).

9. Algèbre linéaire : les fonctions de matrices (exponentielle et logarithme) et la résolution de systèmes matriciels algébriques à l'aide de la théorie des bases de Gröbner.

10. Calcul formel appliqué à la géométrie : étude de systèmes dynamiques discrets dans l'espace à l'aide de la théorie des bases de Gröbner.

En conclusion, il est important de souligner que notre laboratoire a obtenu des résultats conséquents dans la majorité des domaines listés plus haut.

4 Production scientifique

4.1 Publications dans les revues avec comité de lecture (2008-2011 et à paraître) [ACL]

Les travaux et publications présentés concernent la période 2008-2011.

[1] **D. ADAM**: Pólya and Newtonian function fields, Manuscripta Math. 126 (2008), no. 2, 231–246.

[2] **D. ADAM**, Y. FARES: Integer-valued Euler-Jackson's finite differences, Monatshefte für Mathematik, 161, 2010 (1), 15-32.

[3] **D. ADAM**: Fonctions à valeurs entières et module de Carlitz, Journal de théorie des nombres de Bordeaux, 22, nr. 2 (2010), 271-286.

[4] **D. ADAM**: Gel'fond-Fridman theorems for $\mathbb{F}_q[T]$, à paraître en 2010 dans la revue *Israel Journal of Mathematics* (référence 5090).

[5] **D. ADAM**, J.-L. CHABERT et Y. FARES: Subsets of $\mathbb{Z}$ with simultaneous orderings, *Integers* 10 (2010), 437-451.

[6] **D. ADAM**, J.-P. CAHEN: Newtonian and Schinzel quadratic fields, *J. of Pure And Applied Algebra*, 215 (2011), 1902-1918.

[7] **D. ADAM**: Polynômes à valeurs entières ainsi que leurs dérivées en caractéristique p, à paraître dans la revue Acta arithmetica.

[8] **S. BALLET**: On the tensor rank of the multiplication in the finite fields. J. Number Theory 128, no. 6, 1795–1806, 2008.

[9] **R. BLACHE, E. FÉRARD**, H.J. ZHU: Hodge-Stickelberger polygons for exponential sums of $P(x^s)$, Math. Res. Lett. 15 (2008), no. 5, 1053–1071.

[10] **G. BOURGEOIS**, J. C. FAUGÈRE: Algebraic attack on NTRU using Witt vectors and Gröbner bases , Journal of Mathematical Cryptology 3 (2009), 205-214.

[11] **G. BOURGEOIS**: Algebraic system theory and Gröbner basis theory. Linear Algebra and Appl., 430 (2009), no. 8-9, 2157 – 2169.

[12] **G. BOURGEOIS**: The matrix equation, $\log(XY) = \log(X) + \log(Y)$: Linear Algebra and its Applications, vol 432 issue (april 2010), 1878-1884.

[13] **G. BOURGEOIS**, S. ORANGE: Dynamical systems of simplices in dimension 2 or 3, in Automated Deduction in Geometry, ADG 2008, Lecture Notes in Computer Science, Volume 6301, p 1-21, Springer, Mai 2011.

[14] **G. BOURGEOIS**: How to solve the equation $XA - AX = f(X)$, Linear Algebra and Appl. 434 (2011), 657-668.

[15] **G. BOURGEOIS**: Pairs of matrices, one of which commutes with their commutator, Electronic Journal of Linear Algebra ISSN 1081-3810, A publication of the International Linear Algebra Society Volume 22, pp. 593-597, June 2011.

[16] **E. FÉRARD**, F. RODIER: Non linéarité des fonctions booléennes données par des polynômes de degré binaire 3 définies sur $\mathbf{F}_{2^m}$ avec m pair, Contemporary Mathematics, vol 521, 41-53, 2010.

[17] **R. OYONO**: Non-hyperelliptic modular Jacobians of dimension 3, Mathematics of Computation 78 (2009), no. 266, 1173-1191.

[18] **R. OYONO**, E. GONZÁLEZ-JIMÉNEZ: Non-hyperelliptic modular curves of genus 3, Journal of Number Theory 130 (2010), pp. 862-878.

[19] F. LUCA, **R. OYONO**: An exponential Diophantine equation related to powers of two consecutive Fibonacci numbers , Proc. Japan Acad. Ser. A Math. Sci. Volume 87, Number 4 (2011), 45-50.

4.2 Communication avec actes dans des congrès Internationaux (2006-2010 et à paraître) [ACTI]

[20] **S. BALLET**: A note on the tensor rank of the multiplication in certain finite fields, Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications, World Sci. Publ., Hackensack, NJ, pp. 332–342, 2008.

[21] **J. CHAUMINE**: Multiplication in small finite fields using elliptic curves, Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications, World Sci. Publ., Hackensack, NJ, pp. 343–350, 2008.

[22] **E. FÉRARD**, F. RODIER: Non linéarité des fonctions booléennes donnés par des traces de polynômes de degré binaire 3, Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications, World Sci. Publ., Hackensack, NJ, pp. 388–409, 2008.

[23] S. FLON, **R. OYONO**, C. RITZENTHALER: Fast addition on non-hyperelliptic genus 3 curves, Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications, World Sci. Publ., Hackensack, NJ, pp. 1 – 28, 2008.

[24] **R. OYONO**, C. RITZENTHALER: On rationality of the intersection points of a line with a plane quartic, proceeding of the international workshop WAIFI 2010 (International Workshop on the Arithmetic of Finite Fields), LNCS 6087, 224-237, 2010.

4.3 Editions

[25] **J. CHAUMINE**: Algebraic geometry and its applications, Proceedings of the first SAGA conference, 7-11 May 2007, Papeete, vol.5, World Scientific, Number Theory and Its Applications, editors J. Hirschfeld, J. Chaumine and R. Rolland, 2008.

4.4 Prépublications, article soumis

[26] **D. ADAM**, Y. FARES: On two like-affine dynamical systems in a local field, *soumis* en Juin 2011 à Journal of Number Theory.

[27] **G. BOURGEOIS**: Algebraic matrix equations in two unknowns, *soumis* en Avril 2011 à Linear Algebra and Applications.

[28] S. BALLET, **J. CHAUMINE**, J. PIELTANT, R. ROLLAND: On the tensor rank of multiplication in finite extensions of finite fields, 2011, arXiv:1107.1184v2.

[29] **E. FERARD, R. OYONO**, F. RODIER : Some More Functions That Are Not APN Infinitely Often. The Case of Gold and Kasami exponents, *soumis* en Aout aux comptes rendus de AGCT 13, 2011.

4.5 Communications dans un colloque International avec comité de lecture (sans Actes)

Gérald Bourgeois :

Juin 2008	Conférence ILAS, Cancun.

Roger Oyono :

Mars 2009	Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc (CHiLe 2009), Puerto Montt, Chile: *On rationality of intersection points of a line with a plane quartic*.
Dec. 2008	7th joint Australia-New Zealand Mathematics Convention (ANZMC 2008), Christchurch, New Zealand: *Modular curves of Genus Three*.

4.6 Communications en colloque international

David Adam :

Mars 2010	Diophantine approximation and related fields: *Gel'fond-Friedman theorem in positive characteristic*.

4.7 Communications sur invitation en école internationale

Roger Oyono :

Avr. 2008	Cours de MASTER (6 heures) à l'Université autonome de Madrid : *The discrete logarithm problem in cryptography*.

4.8 Exposés en Séminaire

David Adam :

Mars 2010 Meiji Gakuin University, *Simultaneous orderings in function fields*.

Jan. 2010 Séminaire d'Algèbre et Théorie des Nombres du LAMFA, Amiens:

- *Polynômes à valeurs entières ainsi que leurs dérivées en caractéristique finie.*
- *Théorème de Gel'fond-Mitropolsky pour* $\mathbb{F}_q[T]$.
- *Fonctions à valeurs presque entières sur le module de Carlitz.*

Roger Oyono :

Avr. 2008 Séminaire de Théorie des Nombres à l'Université autonome de Madrid: *On rationality of intersection points of a line with a plane quartic*.

5 Autres activités liées au métier de chercheur

5.1 Expertise scientifique

Roger Oyono a expertisé un dossier CIFRE (2009).

5.2 Diffusion de la recherche : activités de rapporteur et de reviewer

5.2.1 Rapporteur

David Adam : Rapporteur pour le Journal of Number Theory, rapporteur pour la conférence INDOCRYPT 2011.

Roger Oyono : Rapporteur pour la conférence "CT RSA conference 2006", rapporteur pour les conférences INDOCRYPT 2011, SAC 2008 (Selected Area of Cryptography) et SAC 2011, pour le Journal of Mathematical Cryptology, pour la conférence Eurocrypt 2008 et les revues AAECC, Information Processing Letters et IET Information Security.

5.2.2 Reviewer

David Adam : Reviewer pour la division Mathematical Reviews de l'American Mathematical Society.

Roger Oyono : Reviewer pour la division Mathematical Reviews de l'American Mathematical Society.

5.2.3 Comité d'organisation

Roger Oyono : Membre du comité de programme de SAC 2008 (Selected Area of Cryptography), membre du comité de programme d'INDOCRYPT 2011.

5.3 Partenariat et actions associées

5.3.1 Participation à la vie scientifique de l'Université

Les membres du laboratoire GAATI continueront à mettre leurs connaissances à la disposition de leurs collègues scientifiques. Cet aspect pourra être développé pour une plus grande efficacité.

5.3.2 Conventions

Depuis juin 2001, notre équipe a une convention avec :

L'équipe Arithmétique et Théorie de l'Information de l'Institut de Mathématiques de Luminy (CNRS UMR 6206) et l'Université de la Méditerranée.

5.3.3 Réseaux et groupes de recherche

Notre équipe est Membre du groupe de recherche **GDR Informatique, Mathématique (IM)**, sous groupe **C2 : codage et cryptographie**, dirigé par Claude Carlet.

5.3.4 Collaborations individuelles

Depuis 2001, notre équipe collabore avec :

Yves Aubry : Université de Toulon et du Var, Toulon (83), France.

Stéphane Ballet : Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR 6206), Marseille (13), France.

Paul-Jean Cahen : Université Paul Cézanne Marseille 3, France.

Jean-Luc Chabert : Université de Picardie Jules Verne.

Jean-Charles Faugère : Université Paris VI.

Enrique Gonzalez-Jimènez : Université autonome de Madrid (Espagne).

Hirata-Kohno Noriko : Nihon University (Japon).

Robert Rolland : Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR 6206), Marseille (13), France.

Christophe Ritzenthaler : Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR 6206), Marseille (13), France.

François Rodier : Arithmétique et Théorie de l'Information, Institut de Mathématiques de Luminy (CNRS UMR 6206), Marseille (13), France.

Igor Shparlinski : Macquarie University (Australie).

Nicolas Thériault : Universidad del Bio-Bio, Concepcion (Chili).

Florian Luca : Institut mathématique de l'Université de Mexico (UNAM, Morelia, Mexico).

5.3.5 Missions associées

Ces différents types de partenariat ont débouché sur plusieurs missions des membres de notre équipe et vice versa (dont l'aboutissement a été plusieurs travaux en collaboration) :

- **Jean Chaumine** a effectué deux missions (2008, 2009) à l'Institut de Mathématiques de Luminy (Marseille).
- **Roger Oyono** a effectué une mission en Mai 2008 (1 semaine) à l'Institut de Mathématiques de Luminy, deux missions (en Mars 2009 (2 semaines) et en Janvier 2011 (3 semaines)) à l'Université de Talca, une mission en Avril 2009 (2 semaines) à l'université autonome de Madrid.
- **Yves Aubry** a effectué une mission en Janvier 2011 (2 semaines) à l'UPF.
- **Florian Luca** a effectué une mission en Novembre 2010 (2 semaines) à l'UPF.
- **Stéphane Ballet** a effectué une mission en Mars 2010 (2 semaines) à l'UPF.
- **Nicolas Thériault** a effectué deux missions en Janvier 2008 (3 semaines) et en Septembre 2011 (2 semaines) à l'UPF.

5.3.6 Evolutions possibles des collaborations

Actuellement il existe un certain nombre d'universités du Pacifique susceptibles d'être intéressées par une collaboration ou un partenariat avec notre équipe tels que Macquarie University, The University of the South Pacific, Hawaian University, Universidad del Bio-Bio, University of Auckland dans la mesure où elles hébergent des équipes de recherche dans des domaines connexes voire identiques à notre domaine de recherche. Pour certaines, des relations de travail existent déjà.

6 Responsabilités collectives et activités administratives

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

6.1 Général

6.1.1 Echelon national

Jean Chaumine :

• Membre du jury du CAPES Français-Tahitien option Mathématiques, 2008-2009.

Jean-Marie Goursaud :

• Membre du jury du CAPES Français-Tahitien option Mathématiques, correction de l'épreuve écrite, 2009-2010.

6.1.2 Echelon local

Jean-Marie Goursaud :

• Membre titulaire du Conseil d'Administration de l'UPF, 2008-2010.

Jean Chaumine :

• Membre du comité de sélection de l'UPF, 2008-2009.

• Membre titulaire du Conseil Scientifique, 2008-2009.

Eric Ferard :

• Membre du comité de sélection de l'UPF, 2008-2009.

6.2 Enseignement

Jean Chaumine :

• Enseignant référent depuis 2008.

• Responsable pédagogique du "Master enseignement", 2010-2011.

David Adam :

• Responsable pédagogique de la 3ème année (MI), 2010-2011.

Eric Férard :

• Responsable pédagogique de la 3ème année (MI), 2003-2010.

• Enseignant référent depuis 2008.

Jean-Marie Goursaud :

• Enseignant référent depuis 2008.

• Chargé de mission de la vie étudiante de l'UPF, 2005-2009.

• Vice-Président des études et de la vie étudiante de l'UPF, depuis 2009.

Roger Oyono :

• Responsable pédagogique de la 2ème année (MI), depuis 2009.

• Enseignant référent depuis 2008.