

Rapport d'Équipe 2000–2005

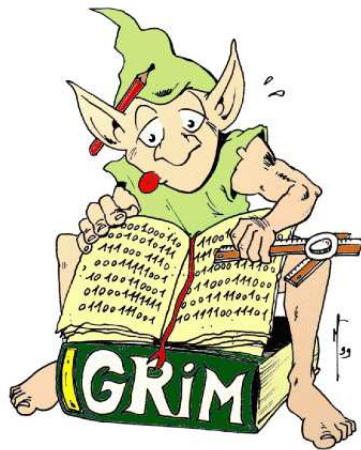
Université du Sud Toulon-Var, Faculté des Sciences et Techniques

Groupe de Recherche  
en  
Informatique et Mathématiques

PPF-STIC-GRIM

[grim@univ-tln.fr](mailto:grim@univ-tln.fr)  
<http://grim.univ-tln.fr>

Directeur : Philippe Langevin



## CONTENTS

1. Historique	3
2. Liste des membres	4
3. Perspectives	5
4. Projets	6
5. Publications et travaux	8
Articles de revues internationales avec comité de lecture	8
Actes de proceedings internationaux avec comité de lecture	9
Ouvrages	9
Contrats de recherche	9
Conférences internationales avec comité de lecture	9
Ecoles et Conférences nationales	10
6. Le séminaire régional Azurcrypt	12
7. Le colloque international YACC	13
8. Autres évènements organisé par des membres de l'équipe	14
9. Fiches individuelles	14

## 1. HISTORIQUE

Le Groupe de Recherche en Informatique et Mathématiques (**GRIM**) est une équipe de recherche de la faculté des sciences et techniques de l'université de Toulon. Historiquement, il s'agit d'un laboratoire de mathématiques (**GECT**) créé par Jacques Wolfmann dans les années quatre-vingt. Au cours de la période de recrutement d'enseignants-chercheurs de la section 27, le **GECT** a initié et favorisé le recrutement d'informaticiens d'horizon divers : bases de données, logique et image sur le site de Toulon. Le Groupe d'Étude de Codage de Toulon est alors constitué de deux équipes : l'équipe **SIS** (dir: Jacques Lemaitre ) et l'équipe **CODE** (dir: Jacques Wolfmann ) qui se sont séparées en deux laboratoires au milieu des années quatre-vingt-dix. Le **GRIM** est issu de l'équipe **CODE**. Il est important de noter que pendant toute cette période, le laboratoire **GRIM** n'a jamais eu de difficulté à être reconnu par les différentes directions scientifiques (mathématique et informatique) du Ministère. Le **GRIM** a perdu son label d'équipe d'accueil EA-1355 lors de la dernière évaluation pour être inséré dans le plan PPF-STIC de l'université de Toulon pour deux ans, avec pour mission d'intégrer une structure plus importante à mi-parcours du plan quadriennal 2006.

<b>AAA</b>	Antilles	J.-P.Cherdieu	<b>A2X</b>	Bordeaux	C. Bachoc
<b>GREYC-LMNO</b>	Caen	B. Vallé	<b>ENS</b>	Paris	D. Pointcheval
<b>MIR-ENST</b>	Paris	G. Cohen	<b>ENSTA</b>	Paris	P. Loidreau
<b>CODE-INRIA</b>	Rocquencourt	N. Sendrier		Grenoble	R. Gillard
<b>LIFL</b>	Lille	F. Recher	<b>LACO</b>	Limoges	T. Berger
<b>ATI-IML</b>	Luminy	R. Rolland	<b>LATP</b>	Marseille	P. Liardet
<b>LIRMM,I3M</b>	Montpellier	J-C. Bajard	<b>CRAN</b>	Nancy	G. Bloch
<b>I3S,INRIA</b>	Nice	P. Solé	<b>LIX</b>	Paris	F. Morain
<b>MAATICAH</b>	Paris	C. Carlet	<b>LGATI</b>	Polynésie	S. Ballet
	Rouen	J.F. Michon	<b>SIS</b>	Toulon	S. Harari
<b>GRIM</b>	Toulon	P. Langevin	<b>GRIMM</b>	Toulouse	T. Henocq
	Toulouse	A. Poli		Versailles	J. Patarin

FIGURE 1. Équipes du groupe **C2** (localisation et correspondants): **mathématique**, **math-info** et **informatique**. Les activités de codage et de cryptographies constituent une véritable activité interdisciplinaire.

Le **GRIM** fait partie du groupe de travail **C2** du GDR **ALP** Algorithmique, Logique et Programmation. Le groupe **C2** (sous la responsabilité de Claude Carlet) est composé d'une quinzaine d'équipes. La communauté **C2** regroupe l'ensemble des chercheurs mathématiciens et/ou informaticiens intéressés par le codage et la cryptographie [1].

Au cours du précédent quadriennal, le **GRIM** s'est fixé comme priorité de s'impliquer dans la structuration de la recherche en codage & cryptographie aux niveaux: régional, national et international. Nous avons mis en place un séminaire régional important (**AZURCRYPT**) financé par une **ACI**-cryptologie. Des subventions de la région et du pôle technologique de l'université ont permis l'organisation d'une conférence internationale (**YACC**). Ces deux actions sont devenus des rendez-vous importants de la "communauté" qui s'intercalent parfaitement entre la conférence **WCC** organisée par le projet code de **INRIA**, le colloque **AGCT** de l'**IML**, les journées **JC2** du GDR, et le séminaire **CCA** de l'**ENSTA**.

Il est important de noter que tous les membres du laboratoire ont contribué à la mise en place de ces nouvelles activités.

## 2. LISTE DES MEMBRES

La double compétence mathématique-informatique est une des caractéristiques du GRIM. L'équipe est en effet composée de mathématiciens et d'informaticiens. Certains des chercheurs du laboratoire ont été qualifiés dans les sections 25, 26 et 27 par les experts du CNU.

*Titulaires*

Yves	AUBRY <sup>1</sup>	HDR	27
Philippe	LANGÉVIN <sup>2</sup> ,	PR	27
Valérie	GILLOT	MC	27
Christian	NGUYEN	MC	27
Patrice	RABIZZONI	MC	27
Pascal	VERON	MC	27
Jacques	WOLFMANN <sup>3</sup>	PR	27
Jean-Pierre	ZANOTTI	MC	27

*Doctorants*

Patrick	LACHARME	AM	
Julien	BRINGER <sup>4</sup>	AMN	

*Secrétariat:*

Corinne	VERA <sup>5</sup>		
---------	-------------------	--	--

---

<sup>1</sup>Dernier arrivant.

<sup>2</sup>Directeur de l'équipe.

<sup>3</sup>En activité jusqu'au 31 août 2006, éméritat demandé à partir du 1er septembre 2006.

<sup>4</sup>Recherche et développement SAGEM.

<sup>5</sup>Secrétaire patargée : Phymat, ANLA, GRIM, dpt Physique.

### 3. PERSPECTIVES

Ces quatre dernières années, tous les membres du **GRIM** se sont investis dans des questions de natures cryptographiques. Au niveau de la recherche : tatouage des images, contrat d'études sur les fonctions booléennes, articles et conférences sur les fonctions courbes, ouvrages. Au niveau de la structuration de la recherche : séminaire régional et conférence internationale. Au niveau de l'enseignement : cours de codage et cryptographie dans les seconds et troisièmes cycles. Au niveau de la vulgarisation scientifique : participation régulière aux «fêtes de la sciences», documents électroniques sur le web. L'ensemble de ces activités témoignent et donnent lieu à des collaborations avec la plupart des acteurs de la cryptographie de la région académique et industriels.

#### Collaborations

L'objectif du laboratoire pour la prochaine décennie est de consolider les collaborations avec les industriels sur le modèle des relations actuelles entre le **GRIM** et **STMicroelectronic** : nouveaux sujets de recherche, financement de thèses, contrats de recherche. Le laboratoire est interlocuteur privilégié quand il s'agit de mettre en oeuvre des actions où la triple compétence codage-cryptographie-image est primordiale comme par exemple dans la gestion des flux vidéo, des mémoires ou encore des architectures sécurisées. L'équipe est inscrite dans deux actions d'envergures : pôle de compétence industriel, et agence nationale de la recherche. Le **GRIM** représente la composante codage-cryptographie du pôle de compétence solutions communicantes sécurisées **SCS** initié par le **L2MP**. Il représente la composante codage-cryptographie du dossier **ANR** construit autour de l'équipe **ATI** dans le cadre de l'agence nationale de la recherche.

04	H. Dobbertin	←	<b>ITSC</b> Bochum	2	04	J. Wolfmann	→	Mexico	2
05	G. Leander	←	<b>ITSC</b> Bochum	2	05	P. Langevin	→	<b>ITSC</b> Bochum	2
05	O. Mbodj	←	Sénégal	4	05	J.-P. Zanotti	→	<b>ITSC</b> Bochum	2
06	G. MacGuire	←		4	04	J. Wolfmann	→	<b>UNAM</b> , Mexico	2

FIGURE 2. visites et échanges: année, chercheur, lieu et durées en semaine.

#### Invitations

Le laboratoire utilise régulièrement les mois d'invités sur poste vacants de l'**USTV** pour inviter des chercheurs étrangers. Un programme d'invitations réciproques entre le **GRIM** et le centre **ITSC** de H.Dobbertin est en cours pour développer un travail commun dans le domaine des fonctions courbes.

#### Formation

Dans le cadre de la réforme 3-5-8, le **GRIM** est associé avec le **LSIS** pour proposer une formation de master (**master sis**) au niveau 4 et 5 incluant les thématiques du laboratoire.

Au niveau 2 et 3, le laboratoire a fortement contribué à l'émergence d'un parcours **Informatique & Mathématiques** au sein de la Faculté des Sciences. Il s'agit d'offrir une formation à la double compétence en Mathématiques et Informatique. L'équipe intervient dans les enseignements de troisième cycle de Toulon (**SIS**) et de Luminy (**MDFI**).

## thèses & hdr

Y. AUBRY

J. BRINGER, *Contribution à l'étude de l'utilisation des codes en cryptographie*, dirigée par P. Langevin.

P. LACHARME, *Renforcement cryptographique des générateurs aléatoires*, direction : P. Langevin et P.-Y. Liardet ([STMICROELECTRONIC](#))

## 4. PROJETS

Les projets de l'équipe s'articulent autour de quatre thèmes qui, sur la base de l'existant (invitation, projet ANR, convention de recherche), donneront lieu, à des collaborations plus ou moins importantes avec des chercheurs extérieurs : l'équipe de Horacio Tapia-Recillas département de mathématique de UMAI au Mexique, l'équipe [ITSC](#) de Dobbertin à Bochum en Allemagne, l'équipe [ATI](#) de Gilles Lachaud, Oumar Mbodj du département de mathématique de l'UGB à Saint-Louis au Sénégal, unité de cryptologie de Pierre-Yvan Liardet du groupe STMICROELECTRONICS.

<i>Thématique:</i>			
Fonctions booléennes	Variétés algébriques	Codes Cycliques	Images et cryptographie
<i>Fondement théorique:</i>			
théorie des groupes, sommes exponentielles, géométrie algébriques	algorithmique et géométrie algébrique	théorie des nombres, des corps et des anneaux finis	Algorithme théorie des graphes
<i>Application:</i>			
chiffrement à flots générateurs aléatoires	cryptographie à clef publique, codes géométriques	codage et synchronisation	indexation watermarking

FIGURE 3. Projets de recherches.

### Fonctions booléennes

*participant(e)s:* V. Gillot, P. Lacharme, Ph. Langevin, P. Rabizzoni, P. Véron, J.-P. Zanotti. Le projet concerne l'étude des fonctions booléennes dans le contexte de la cryptographie à clef secrète, du codage et des générateurs aléatoires. Rappelons que l'étude des fonctions booléennes est primordiale dans le cadre de la cryptographie à clef secrète ; elles sont (par exemple) utilisées pour combiner la sortie de registres à décalage au coeur des mécanismes de chiffrement à flot. L'action "Fonctions booléennes" que nous proposons se décline en plusieurs axes.

- fb<sub>1</sub>** Le premier consiste en l'étude des fonctions booléennes invariantes sous l'action de certains groupes. L'évaluation de sommes exponentielles (incomplètes) associées à certaines variétés algébriques nous permet d'exhiber des classes de fonctions hautement non-linéaires, ce qui constitue le principal point d'attaque de [3] de la conjecture de Patterson et Wiedemann.
- fb<sub>2</sub>** Dans le prolongement de [13], l'objectif du deuxième axe est de déterminer les 999 classes de formes binaires homogènes de degré 4 en 8 variables dans le but d'estimer le rayon de recouvrement du code de Reed-Muller  $RM(3, 8)$  mais aussi d'estimer le nombre de fonctions courbes en 8 variables.
- fb<sub>3</sub>** Pour résister aux différentes cryptanalyses, les fonctions booléennes et vectorielles mises en jeu doivent respecter un strict cahier des charges. Les critères théoriques de celui-ci sont principalement : la non-linéarité, l'équilibre de la fonction, un degré du polynôme associé élevé et une résistance aux attaques par corrélation et attaques algébriques... L'objectif du troisième axe consiste à interpréter ces questions dans le cadre du chiffrement à la volée [1] et de la construction de générateurs aléatoires sûrs [1].

### Variétés algébriques.

*participants: Y. Aubry, Ph. Langevin, P. Véron.*

- va<sub>1</sub>** La construction par Goppa de codes définies sur des courbes algébriques a permis d'exhiber des familles infinies de codes linéaires dépassant la borne de Varshamov-Gilbert. Nous nous proposons de poursuivre nos propres travaux sur l'étude des codes géométriques construits à partir de surfaces algébriques.
- va<sub>2</sub>** Les sommes de Gauss sont des entiers algébriques présents dans de nombreuses questions et le calcul effectif de celles-ci est très important. Nous élaborerons un programme pour calculer ces sommes sur des extensions de degré élevé (de l'ordre de 40) sur le corps à 2 éléments. Elles sont liées aux courbes d'Artin-Schreier qui nous entraînent vers la formule de Gross-Koblitz qui fait intervenir la fonction Gamma p-adique. Il s'agit d'obtenir un algorithme efficace pour estimer les valeurs de la fonction Gamma.
- va<sub>3</sub>** L'utilisation des variétés abéliennes, essentiellement les courbes elliptiques et les jacobiniennes de courbes hyperelliptiques, est apparue en cryptographie pour faire émerger des classes de groupes pour lesquels on ne connaît pas d'algorithmes sous-exponentiels pour résoudre le problème du logarithme discret. Nous proposons d'étudier les problèmes posés par l'implantation de protocoles à base de courbe elliptiques.

### Codes cycliques.

*Participant(e)s : Y. Aubry, V. Gillot, Ph. Langevin, C. Nguyen, P. Rabizoni, J. Wolfmann, J.-P. Zanotti.*

**cc<sub>1</sub>** La détermination des distributions des poids des codes cycliques irréductibles binaires est un problème classique et fascinant de la théorie des codes. Par exemple, on ne sait toujours pas caractériser les codes cycliques irréductibles binaires à deux poids. Une conjecture affirme que les codes cycliques binaires irréductibles sont de type semi-primitif. Nous travaillons sur cette conjecture avec les outils que nous propose la théorie algébrique des nombres.

**cc<sub>2</sub>** Des résultats spectaculaires ont été obtenus en considérant des codes sur l'anneau  $\mathbb{Z}/4\mathbb{Z}$ . Il convient maintenant d'étudier de manière systématique les constructions de codes, séquences, designs etc, non plus sur les corps mais sur les anneaux finis. Nous poursuivons ces recherches dans le but de construire des fonctions booléennes hautement non linéaires.

**cc<sub>3</sub>** Nous avons faits de nombreuses expérimentations numériques dans le cadre de l'étude des fonctions booléennes, des codes cycliques binaires et des séquences idéalement corrélées. Nous disposons de plusieurs milliers de lignes de code en langage C que nous envisageons de fondre en une bibliothèque de calculs spécifique au mode binaire.

### Images et graphes.

*Participants: Ph. Langevin, C. Nguyen et J.-P. Zanotti*

**ig<sub>1</sub>** La segmentation permet d'associer un graphe planaire à une image : le graphe des régions. Nous nous intéressons aux transformations géométriques qui laissent invariante la classe d'isomorphismes géométriques sous certaines conditions d'une image.

**ig<sub>2</sub>** Les résultats actuels en matières de watermarking sont encore très sensibles aux attaques de type géométrique. Nous nous proposons d'étudier la résistance d'une signature intégrée à une image caractérisée par un graphe planaire à de telles attaques.

## 5. PUBLICATIONS ET TRAVAUX

Dans les listes qui suivent, un astérisque (\*) sur une publication signifie une publication «acceptée» et «à paraître» dans l'année.

### ARTICLES DE REVUES INTERNATIONALES AVEC COMITÉ DE LECTURE

- [1] G. Vega and Jacques Wolfmann. Some families of  $\mathbb{Z}_4$ -cyclic codes. *Finite Field and Their Application*, 10:530–539, 2004.
- [2] Philippe Langevin and Jean-Pierre Zanotti. Finite groups and highly non-linear Boolean functions. *Design codes and cryptography*, 46(2):131–146, 2005.
- [3] Yves Aubry and M. Perret. Divisibility of zeta functions of curves in a covering. *Archiv der Math*, 82:205–213, 2004.

- [4] Yves Aubry and Marc Perret. On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields. *Finite Fields and Their Applications*, 10(3):412–431, 2004.
- [5] Philippe Langevin and Pascal Véron. Non-linearity of power functions. *Designs, codes and cryptography*, 37(1), 2005.
- [6] Philippe Langevin and Patrick Solé.  $Z_4$  duadic codes. *Finite Fields and Applications*, 6:309–326, 2000.
- [7] Yves Aubry. Class number in non Galois quartic and non Abelian Galois octic function fields over finite fields. *Bulletin of the Greek Math. Soc.*, 2005\*.
- [8] Pascal Véron. True dimension of some quadratic binary trace Goppa codes. *Design, Codes and Cryptography*, 24:81–97, 2001.
- [9] Pascal Véron. Proof of conjectures on the true dimension of some binary Goppa codes. *Designs codes and cryptography*, 31(1):31–44, 2005.
- [10] Jacques Wolfmann. Negacyclic and cyclic codes over  $Z_4$ . *IEEE Trans. Inform. Theory*, 45:2527–2532, 1999.
- [11] Jacques Wolfmann. Difference sets in  $Z_4^m$  and  $F_2^{2m}$ . *Designs, Codes and Cryptography*, 20:73–88, 2000.
- [12] Jacques Wolfmann. Binary images of cyclic codes over  $Z_4$ . *IEEE Trans. Inform. Theory*, 47:1773–1779, 2001.
- [13] Jacques Wolfmann. Are 2-weight projective cyclic codes irreducible? *IEEE Trans. Inform. Theory*, 2005.

#### ACTES DE PROCEEDINGS INTERNATIONAUX AVEC COMITÉ DE LECTURE

- [1] Ph. Langevin and J.-P. Zanolli. Around the counter example of Paterson and Wiedemann. pages 214–229. *Finite Fields Fq6*, 2002.
- [2] Ph. Langevin Ph. and P. Solé. Gauss sums over quasi-Frobenius rings. pages 329–341. *Finite fields Fq5*, 2001.
- [3] J. Bringer and V. Gillot and Ph. Langevin. Exponential sums and Boolean functions. In *BFCA '05*, 2005\*.

#### OUVRAGES

- [1] Yves Aubry and Gilles Lachaud. *Arithmetic, Geometry and Coding Theory*, volume 11 of *séminaires et congrès*. smf edition.
- [2] Pierre Barthélemy and Robert Rolland and Pascal Véron. *Cryptographie : Principes et mises en œuvres*. 2005.

#### CONTRATS DE RECHERCHE

- [1] Patrice Rabizzoni and Pascal Véron. Expertise et amélioration d'un système de chiffrement utilisant des codes correcteurs pour une EEPROM. Technical report, STMicroelectronics, 2005. 15 Keuros.
- [2] Valérie Gillot and Patrice Rabizzoni and Jacques Wolfmann. Fonctions booléennes hautement non-linéaires équilibrées et codes cycliques quaternaires. Technical report, DCSSI, Service du chiffre, 2001. 145 KF.

#### CONFÉRENCES INTERNATIONALES AVEC COMITÉ DE LECTURE

- [1] Jérôme Folli and Christian Nguyen. Watermark under graph. In *GRETSI 2003, XIX*, page 283. Traitement du signal et des images.
- [2] Philippe Langevin and Patrick Solé. Duadic  $z_4$ -codes. In *ISIT 2000*. IEEE international symposium on Information Theory, 2000.
- [3] Philippe Langevin and Patrick Solé. Gauss sums over quasi-frobenius rings. In *Fq5*, Augsburg, Allemagne, 2000. *Finite Fields and Applications*.

- [4] Yves Aubry and Philippe Langevin. On the weight of irreducible cyclic codes. In *Workshop on Coding Theory and Cryptography*, Bergen, Norway., mars 2005.
- [5] Yves Aubry. Divisibility of zeta functions in a covering of curves. In *AGCT-8*, Marseille, France, 2001. IML.
- [6] Yves Aubry. Number of rational points of connected projective algebraic curves. In *Fq6*, Oaxaca, Mexico., 2001. Finite Fields and Applications.
- [7] Yves Aubry. Géométrie algébrique et borne de Gilbert-Varshamov. In *Ecole internationale Codes correcteurs d'erreurs et cryptographie*, Dakar, Sénégal, mars 2003.
- [8] Yves Aubry. Zeta functions and bounds "à la Weil". In *AGCT-9*, Marseille, France, mai 2003. IML.
- [9] Yves Aubry. Zeta functions of connected curves over finite fields. In *Workshop Computational aspects of algebraic curves and cryptography*, Floride, USA, mars 2003. IML.
- [10] Julien Bringer. Non linearity of some paterson-wiedemann type functions. In *yacc-04*, Porquerolles, june 2004. GRIM.
- [11] Jacques Wolfmann Gerardo Vega. some classes of cyclic codes over  $Z_4$ . In *Fq7*, Toulouse, France, 2003. Finite Fields and their Applications.
- [12] Valérie Gillot and Philippe Langevin Julien Bringer. Exponential sums and boolean functions. In *BFCA'05*, Rouen, 2005.
- [13] Éric Brier E. and Philippe Langevin. The classification of boolean cubics of nine variables. In *2003 IEEE Information Theory Workshop*, "La Sorbonne", Paris, France.
- [14] Philippe Langevin. About the counter-example of Patterson et Wiedeman. In *Fq6*, Oaxaca, Mexico., june 2001. Finite Fields and Applications.
- [15] Philippe Langevin. Nonlinearity of power functions. In *AGCT-8*, Luminy, France, 2001. IML. Conférencier invité.
- [16] Philippe Langevin. Classification of boolean cubics of 9 variables. In *Arithmétique et Combinatoire*, Luminy, France, 2002.
- [17] Philippe Langevin. Nonlinearity of power functions. In *yacc-02*, Porquerolles, France, 2002. GRIM.
- [18] Philippe Langevin. correlation of sequences. In *Ecole internationale : suites pseudo-aléatoires*, Manille, Philippines, juillet 2005. CIMPA.
- [19] Gregor Leander Philippe Langevin. Monomial bent functions. In *AGCT-10*, Marseille, France., September 2005. IML.
- [20] Pascal Véron. Twenty years of cryptography and error-correcting codes. In *SCI'2000*, Orlando, USA, 2000. Finite Fields and Applications.
- [21] Pascal Véron. Proof of conjectures on the true dimension of some binary goppa codes. In *Fq6*, Oaxaca, Mexico., 2001. Finite Fields and Applications.
- [22] Pascal Véron. Systèmes de fichiers distribués sécurisés. In *JRES'03*, pages 211–226, 2003.
- [23] Jacques Wolfmann. Binary cyclic codes which are  $z_4$ -cyclic codes. Washington, USA, 2001. I.E.E.E. International Symposium on Information Theory.
- [24] Jacques Wolfmann. Binary images of cyclic codes over  $z_4$ . In *WCC*, Paris, France, 2001. WCC.
- [25] Jacques Wolfmann. Cyclic codes over  $z_4$ , their binary images and related objects. Luminy, France, 2001. IML.
- [26] Jacques Wolfmann. Bent functions as polynomials over  $z_4$ . San Diego, USA, 2002. SIAM Conference on Discrete Mathematics.
- [27] Jacques Wolfmann. 2-weight projective cyclic codes. In *Workshop on Coding Theory and Cryptography*, Bergen, Norway., 2005.
- [28] Philippe Langevin Yves Aubry. Cyclic codes with few different weights. In *AGCT-10*, Marseille, France., September 2005. IML.
- [29] Jean-Pierre Zantotti. Finite groups and highly non-linear boolean functions. In *Fq6*, Oaxaca, Mexico., 2001. Finite Fields and Applications.

#### ÉCOLES ET CONFÉRENCES NATIONALES

- [1] Patrick Lacharme. Générateurs aléatoire sécurisé. In *Journées Codage et Cryptographie*, Aussois, Savoie, Janvier 2005. ALP-C2.

- [2] Philippe Langevin. Corrélations et séquences. In *Journées Codes et Cryptographie*, Marseille, France., 2002. ALP-C2.

## 6. LE SÉMINAIRE RÉGIONAL AZURCRYPT

L'équipe anime le séminaire [AZURCRYPT](#) proposé par le [GRIM](#), retenu et subventionné par l'ACI-Cryptographie du ministère de la recherche. Le séminaire est sous la responsabilité de Pascal Veron. Pour l'essentiel, il s'agit de structurer et de promouvoir la recherche en cryptographie dans le sud de la France au moyen d'un séminaire quadriannuel ouvert aux entreprises de la région PACA et animé par les équipes de recherche des universités voisines:

labo.	équipe		localisation
IML	ATI	Arithmétique et Théorie de l'Information	Aix-Marseille II
LATP	DSA	Dynamique Stochastique et Algorithmique	Aix-Marseille I
GRIM		Groupe de Recherche en Info. et Math.	Toulon
LIF	MOVE	Modélisation et Vérification	Aix-Marseille I

Afin de constituer un véritable lieu d'échanges, l'orientation de ce séminaire s'efforce de suivre deux axes complémentaires : l'un théorique et l'autre pratique. Dans cette optique, les entreprises ont été sollicitées pour effectuer un exposé à chaque réunion afin d'exprimer leurs besoins et leurs attentes quant à une collaboration avec une équipe de recherche. L'organisation de ces rencontres ainsi que le contact avec les différentes entreprises sont assurés par le [GRIM](#). Dans le but de créer une dynamique de groupe, les séminaires se déroulent alternativement sur les différents sites d'accueil de chacune des équipes. Une quinzaine de personnes assistent régulièrement aux réunions.

P. Véron (GRIM)	P.-Y. Liardet (STMic.)	R. Rolland (ATI)
M. Joye (Gemplus)	R. Amadio (Move)	J.-L. Lanet (Gemplus)
P. Liardet (DSA)	Y. Loisel (SCM.)	P. Solé (I3S Nice)
F. Arnault (LACO)	P. Guillot (Canal +)	Y. Teglia (STMic.)
J.-C. Bajard (LIRMM)	M. Joye (Gemplus)	J. Stern (Liens, ENS)
J.-L. Dugelay (Eurecom)	D. Lubicz (Celar)	M. Finiasz (INRIA)
P. Urien (ENST)	S. Harari (SIS)	P. Loidreau (Ensta)
P. Gaborit (LACO)	M. Girault (FT)	M. Virat (U. Nice)
J. Segal (IUFM-ENS)		

FIGURE 4. Liste des conférenciers du séminaire [AZURCRYPT](#) période 2001–2005. ([détail des conférences](#))

## 7. LE COLLOQUE INTERNATIONAL YACC

L'objectif des conférences [YACC](#) est de favoriser la rencontre de chercheurs français, mathématiciens et informaticiens, avec des cryptologues internationalement reconnus, et des chercheurs industriels. Les deux premières éditions se sont déroulées en 2002 et 2004. Une cinquantaine de chercheurs ont participé à la première édition et 75 à la seconde en 2002. Du point de vue financier, ces rencontres sont subventionnées par le Conseil Régional PACA, le Pôle Technologique de l'Université de Toulon, le Conseil Scientifique de l'Université de Toulon et le [GRIM](#).

Le colloque a été logé au centre IGESA dans l'île de Porquerolles. C'est un centre qui dépend des oeuvres sociales de l'armée, entièrement équipé pour l'hébergement et les conférences.

L'organisation a été entièrement prise en charge par les membres du GRIM.

**Yet Another Conference on Cryptography  
International Colloquium on Cryptography and related topics  
Colloque International sur la Cryptographie et sujets connexes  
Ile de Porquerolles, France**

**yacc<sup>02</sup> 3-7 juin 2002**

**yacc<sup>04</sup> 1-5 juin 2004**

*Comité Scientifique :*

A. Canteaut	INRIA, Paris.
J.-M. Couveignes	Univ. Toulouse.
Ph. Langevin	GRIM, Toulon.
P.-Y. Liardet	STM., Marseille.
J. Stern	ENS, Paris.
J. Wolfmann	GRIM, Toulon.

*Comité Scientifique :*

A. Canteaut	INRIA, Paris.
J.-M. Couveignes	Toulouse.
Ph. Langevin	GRIM, Toulon.
P.-Y. Liardet	STMicro., Marseille.
J. Stern	ENS, Paris.

*Conférenciers invités:*

A. Canteaut	INRIA, Paris
J.M. Couveignes	Toulouse
R. Cramer	Denmark
H. Dobbertin	Germany
B. Preneel	Belgium
J. Stern	ENS, Paris
P. Stevenhagen	Netherland

*Conférenciers invités:*

A. Canteaut	Paris.
W. Meier,	FH aargau Suisse.
I. Shparlinski	Australie
J. Stern	ENS, Paris.
S. Vaudenay	Suisse.
S. Vladuts	Marseille

[programme yacc-02](#)  
[Booklet yacc-02](#)

[programme yacc-04](#)  
[Booklet yacc-04](#)

## 8. AUTRES ÉVÈNEMENTS ORGANISÉS PAR DES MEMBRES DE L'ÉQUIPE

Les actions décrites dans les deux sections précédentes sont exclusivement dirigées vers la cryptographie. Y. Aubry est co-organisateur des trois manifestations:

*Juin 2005* La 21e édition des [rencontres arithmétiques](#) de Caen.

*Mai 2003* École européenne *Algebraic Geometry and Information Theory* ([GATI](#)), sous l'égide de l'European Science Foundation, au CIRM.

*Mai 2003* La neuvième édition du congrès international *Arithmetic, Geometry and Coding Theory* ([AGCT-9](#)), sous l'égide de l'European Science Foundation, à Luminy.

Par ailleurs, l'équipe organise un séminaire de mathématique-informatique hebdomadaire. Le [programme du séminaire](#) met en évidence le spectre d'intérêts de l'équipe.

## 9. FICHES INDIVIDUELLES

Philippe [LANGEVIN](#), 43 ans.

*Diplôme:*

1988 Agrégation de mathématiques.

1992 Doctorat de Mathématiques, université de Limoges

2000 HDR, université de Toulon et du Var

*Position:*

2002– PR Informatique, université du Sud Toulon-Var

1998–2000 Délégation C.N.R.S. I3S Nice

1992–2002 MCF Informatique, université de Toulon et du Var.

*Recherche:*

sommes de caractères, équation algébrique, sommes de Gauss, séquences, structures algébriques finies.

*Enseignements:*

algorithmique, programmation, combinatoire algébrique..

*Travaux:*

revues [\[5\]\[2\]](#), proceedings [\[3\]\[1\]\[2\]](#)

\* \* \*

Yves [AUBRY](#), 39 ans.

*Diplôme:*

1993 Doctorat de Mathématiques (Aix-Marseille II)

2002 HDR Aix-Marseille II

*Position:*

2004– MCF Informatique, université du Sud Toulon-Var.

2000–2004 Délégation C.N.R.S. Institut de mathématiques de Luminy.

1993–2000 MCF Mathématiques, université de Caen.

*Recherche:*

Géométrie algébrique (variétés sur les corps finis), Théorie des nombres, nombres de classes dans les corps de fonctions. codes correcteurs.

*Enseignements:*

Mathématiques discrètes

*Travaux:*

revues [7] [3] [4], conférence [4], ouvrage [1].

\* \* \*

Valérie GILLOT, 38 ans.

*Diplôme:*

1993 Doctorat de Mathématiques et Informatique, université de Toulon.

*Position:*

1990–1993 Allocataire moniteur Aix-Marseille II

1993–1994 A.T.E.R. Aix-Marseille I

1994 MCF Informatique, université du Sud Toulon-Var

*Recherche:*

sommes d'exponentielles, fonctions booléennes.

*Enseignements:*

Théorie des langages, programmation, programmation O.O.

*Travaux:*

proceedings [3], contrat de recherche [2].

\* \* \*

Christian NGUYEN, 40 ans.

*Diplôme:*

1993 Doctorat Informatique, université de Nice-Sophia Antipolis.

*Position:*

1994– MCF Informatique, université du Sud Toulon-Var

1988-1991 Allocataire MRT - I3S, Sophia Antipolis.

1992-1993 A.T.E.R. - ESSI, Sophia Antipolis.

1993-1994 A.T.E.R. - U.F.R. Sciences, Nice.

*Recherche:*

watermarking.

*Enseignements:*

infographie, interface homme-machine, programmation orientée objet.

*Travaux:*

conférence [1]

\* \* \*

Patrice RABIZZONI, 55 ans.

*Diplôme:*

1983 Doctorat de Mathématiques Appliquées (Aix-Marseille I)

*Position:*

1990– MCF Informatique université du Sud Toulon-Var

1973–1989 Enseignant de mathématiques du secondaire.

*Recherche:*

Fonctions booléennes, chiffrement à la volée, codes correcteurs d'erreurs.

*Enseignements:*

architecture, codage.

*Travaux:*

contrat de recherche [1][2].

★ ★ ★

Pascal VERON, 35 ans.

*Diplôme:*

1995 Doctorat de Mathématiques et Informatique (université de Toulon)

*Position:*

1997–\* MCF Informatique, université du Sud Toulon-Var.

*Recherche:*

cryptographie, sécurité des réseaux, chiffrement rapide, codes de Goppa

*Enseignements:*

cryptographie, réseaux, système.

*Travaux:*

revues [5] [9] [8], ouvrage [2], conférence [22].

\* \* \*

Jacques WOLFMANN, 67 ans.

*Diplôme:*

1978 Doctorat d'Etat université Paris VII.

*Position:*

1981– PR université du Sud Toulon-Var.

*Recherche:*

codes correcteurs, équations sur les corps finis, anneaux finis, séquences.

*Enseignements:*

codes correcteurs, mathématiques discrètes.

*Travaux:*

revues [13][1][12][11] conférence [25].

\* \* \*

Jean-Pierre ZANOTTI, 39 ans.

*Diplôme:*

1995 Doctorat de Mathématiques et Informatique, université de Toulon.

*Position:*

1995– MCF Informatique, université du Sud Toulon-Var.

*Recherche:*

théorie des codes, actions de groupes.

*Enseignements:*

calculabilité, algorithmique, informatique théorique.

*Travaux:*

revue [2], conférence [1].

\* \* \*