RAPPORT D'ACTIVITÉ 2014

PHILIPPE LANGEVIN

Table des matières

1. Identification 2
2. Activités scientifiques 2
2.1. sujets de recherche 2
2.2. publications et production scientifique 2
2.3. travaux récents 3
Publications récentes 4
2.4. recherche en cours 5
Liste des publications 5
3. Encadrement 8
3.1. mémoire de master 8
Liste des Masters 8
3.2. travaux de thèse 8
Liste des Thèses 8
3.3. jury de thèse 9
Liste des Jurys 9
3.4. postdoc 9
Liste des postdocs 9
3.5. invitation 10
Liste des invitations 10
4. Diffusion 10
4.1. communication 10
Liste des conférences 10
4.2. séjour de recherche 12
4.3. arbitrage 12
4.4. animation 12
4.5. Organisation 12
4.6. vulgarisation 12
4.7. projet numérique 13
5. Responsabilité scientifique 13
5.1. comité de selection 13
5.2. responsabilité 13
6. Enseignement 13
6.1. stage 13
— 14

Date: dernière compilation :4 mars 2015.

Liste des publications 15
Liste des conférences 17

1. Identification

Je m'intéresse à la recherche depuis mon adolescence. Mes premiers travaux de lycéen (1980), une mise en oeuvre d'un algorithme de résolution des équations algébriques, ont été primés[1] au *concours scientifique pour les jeunes* organisé par la société Philips et l'académie des sciences. Je suis devenu professeur d'informatique à l'université de Toulon suite à un parcours d'enseignant chercheur standard : CAPES de mathématique (1987), DEA d'informatique de Luminy (1988), agrégation de mathématique option informatique (1989), allocataire moniteur (1990), doctorat et maître de conférences en informatique (1992), délégation CNRS (1997, 1998) habilitation à diriger des recherche (1999), et professeur d'informatique (2002).

Pour l'heure, je m'implique prioritairement dans les activités d'enseignement, de recherche, de gestion et d'encadrement de la recherche. Concernant mes activités de chercheur, j'alterne des périodes de travaux théoriques qui portent sur des problèmes ouverts issus des communications, avec des périodes de travaux plus pratiques où il s'agit de programmer des expérimentations numériques non triviales.

2. Activités scientifiques

2.1. **sujets de recherche.** Chercheur à l'Institut de Mathématiques de Toulon (IMATH), mes sujets de recherches gravitent autour de le la théorie de l'information. Je m'intéresse aux problèmes de mathématiques discrètes utiles aux communications numériques : théorie des codes correcteurs, synchronisation des signaux, cryptographie. L'algorithmique, la programmation, la combinatoire, les transformées de Fourier, les sommes de Gauss et la théorie de Galois jouent un rôle important dans mon approche. L'ensemble de mon activité d'enseignant-chercheur est accessible à partir de mon site internet via l'URL :

. . . . . http ://langevin.univ-tln.fr

2.2. **publications et production scientifique.** Je publie mes travaux dans les revues et les actes de conférences avec une préférence marquée pour les journaux scientifiques.

- Applicable Algebra in Engineering,
- Acta Arithmetica,
- Boolean Function Cryptography and Application,
- Cryptography and Communication,
- Designs Codes and Cryptography,

[1] collaboration avec mon camarade de classe Fabrice Pelestor

Etat Civil	
Nom :	LANGEVIN
Prénoms :	Philippe, Clément, Antoine.
Né le :	23 Mai 1962 à Toulon, France.
Nationalité :	française.
Habilitation	
Titre :	Les sommes de caractères et la formule de Poisson dans la théorie des codes...
Lieu :	université de Toulon
Date de soutenance :	19 Janvier 1999
Doctorat	
Thèse :	rayons de recouvrement des codes de Reed-Muller affines
Directeurs :	Jacques Wolfmann Guy Robin
Lieu :	université de Limoges
Date de soutenance :	13 Mai 1992
Qualifications	
agrégation	1989, option math. info.
DEA	1988, math. info. Luminy.
CAPES	1987 de mathématiques.
maîtrise	1984, univ. de Provence
licence	1983, univ. de Provence

– Glasgow Math Journal,
– IEEE transactions in Information Theory,
– Finite Fields and Theirs Application,
– Journal of Combinatorial Theory,
– Journal of Combinatorial Number Theory,
– Journal of Number Theory,
– Workshop on Coding and Cryptography.

En moyenne deux publications sur les vingt-cinq dernières années : acte de colloque, rapport, ou article de revue.

La liste exhaustive de mes travaux est placée à la fin de cette section. Les collaborateurs partagent pleinement ces travaux. Les noms des auteurs sont rangés par ordre alphabétique.

2.3. **travaux récents.** Les neuf publications des cinq dernières années, 1 acte et 8 articles dont 3 acceptés et 5 publiés concernent deux de mes sujets favoris : les fonctions booléennes pour la cryptographie et les sommes de caractères pour le partage de canal.

Des résultats numériques importants sur la classification des fonctions courbes en 8 variables ont été obtenus. Une dizaine de chercheurs ont participé à cette aventure. Les touches finales ont été réalisées avec

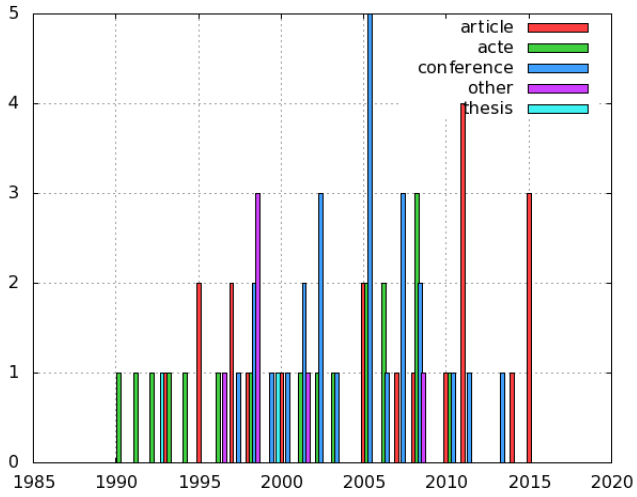

FIG. 1. Travaux, publications et communications.

Gregor Leander et Xiang-Dong Hou. Dans [7], nous avons dénombré le nombre exact de fonctions courbes, un véritable challenge numérique finalisant plusieurs années de recherche. Dans [9], nous avons comptabilisés les fonctions courbes des classes connues. Un résultat qui permet d'envisager l'existence de larges classes de fonctions courbes à découvrir.

Dans [8], nous utilisons des résultats anciens et profonds de la théorie des nombres comme les sommes de Gauss, les congruences de Stickelberger et la formule de Gros-Koblitz pour décrire la fonction duale d'une fonction courbe de type Kasami-Welch.

Avec Yves Aubry et Daniel Katz, nous avons travailler sur deux questions posées par Tor Helleseth dans les années 70. Elles concernent les spectres d'intercorrélation des M-séquences. Dans [5], nous dégageons un résultat assez modeste concernant la divisiblité des somme de Weil qui débouche sur une exitante conjecture adressée dans [2]. Dans [3, 4], nous montrons la formidable efficacité de nos outils en améliorant de manière sensible des résultats de Calderbank, Charpin, McGuire, Helleseth, Poonen et Rubinstein.

Dans un [1], nous résolvons un problème posé en 2001 par Dobbertin, Helleseth, Kumar et Martinsen concernant le spectre de Fourier d'une application monomiale. Une utilisation conjointe de la théorie des graphes et de la théorie des nombre, nous permet de tordre le coup à cette question au moyen des algorithmes de Tarjan et Bellman-Ford !

PUBLICATIONS RÉCENTES

[1] Daniel Katz and Philippe Langevin. Proof of a conjectured three-valued family of weil sums of binomials. *Acta Arithmeticae*, page 20, 2015.

[2] Daniel J. Katz and Philippe Langevin. New open problems related to old conjectures by helleseth. *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences.*, 2015.

[3] Yves Aubry, Daniel Katz, and Philippe Langevin. cyclotomy of Weil sums of binomials. *Journal of Number Theory*, page 20, 2015.

[4] Yves Aubry, Daniel Katz, and Philippe Langevin. cyclotomie des sommes de Weil binomiales. *CRAS Comptes Rendus Mathématique*, 352(5) :373–376, May 2014.

[5] Yves Aubry and Philippe Langevin. On a conjecture of helleseth. In *Algebraic Informatics - 5th International Conference, CAI 2013, Porquerolles, France, September 3-6, 2013. Proceedings*, pages 113–118, 2013.

[6] Yves Aubry, Claude Carlet, Philippe Langevin, and Pascal Véron. Guest editorial for the special issue for jacques wolfmann. *Cryptography and Communications*, 3(4) :187–188, 2011.

[7] Philippe Langevin and Gregor Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes Cryptography 59(1-3)*, 59(1-3) :193–205, 2011.

[8] Philippe Langevin, Gregor Leander, Gary Mcguire, and Eugen Zalinescu. Analysis of kasami-welch functions in odd dimension using stickelberger's theorem. *Journal of Combinatorics and Number Theory*, 2(1) :55 – 72, 2011.

[9] Philippe Langevin and Xiang-Dong Hou. Counting partial spread functions in eight variables. *IEEE Transactions on Information Theory*, 57(4) :2263–2269, 2011.

2.4. **recherche en cours.** mots clefs : fonction courbe, code quantique, code MDS, carré latin, fonction semicourbe, somme de Weil, corrélation de séquences, transformée de Fourier.

Liste des publications

[1] Daniel Katz and Philippe Langevin. Proof of a conjectured three-valued family of weil sums of binomials. *Acta Arithmeticae*, page 20, 2015.

[2] Daniel J. Katz and Philippe Langevin. New open problems related to old conjectures by helleseth. *Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences.*, 2015.

[3] Yves Aubry, Daniel Katz, and Philippe Langevin. cyclotomy of Weil sums of binomials. *Journal of Number Theory*, page 20, 2015.

[4] Yves Aubry, Daniel Katz, and Philippe Langevin. cyclotomie des sommes de Weil binomiales. *CRAS Comptes Rendus Mathématique*, 352(5) :373–376, May 2014.

[5] Yves Aubry and Philippe Langevin. On a conjecture of helleseth. In *Algebraic Informatics - 5th International Conference, CAI 2013, Porquerolles, France, September 3-6, 2013. Proceedings*, pages 113–118, 2013.

[6] Yves Aubry, Claude Carlet, Philippe Langevin, and Pascal Véron. Guest editorial for the special issue for jacques wolfmann. *Cryptography and Communications*, 3(4) :187–188, 2011.

[7] Philippe Langevin and Gregor Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes Cryptography 59(1-3)*, 59(1-3) :193–205, 2011.

[8] Philippe Langevin, Gregor Leander, Gary Mcguire, and Eugen Zalinescu. Analysis of kasami-welch functions in odd dimension using stickelberger's theorem. *Journal of Combinatorics and Number Theory*, 2(1) :55 – 72, 2011.

[9] Philippe Langevin and Xiang-Dong Hou. Counting partial spread functions in eight variables. *IEEE Transactions on Information Theory*, 57(4) :2263–2269, 2011.

[10] Emrah Cakcak and Philippe Langevin. Power permutation in dimension 32. In *Sequences and Theirs Applications - SETA 2010*, volume 6338 of *LNCS*, pages 181 – 188, 2010.

[11] Philippe Langevin and Valérie Gillot. Estimation of some exponential sums by means of weighted degree. *Glasgow Math. Journal*, 52(02) :315–324, 2010.

[12] Philippe Langevin, Gregor Leander, and Gary McGuire. Kasami bent functions are not equivalent to their duals. In *Finite fields and applications*, volume 461 of *Contemp. Math.*, pages 187–197. Amer. Math. Soc., Providence, RI, 2008.

[13] Philippe Langevin and Gregor Leander. Classification of boolean quartic forms in eight variables. In *Boolean Functions in Cryptology and Information Security*, volume 18, pages 139–147, 2008.

[14] Philippe Langevin and Gregor Leander. Monomial bent functions and Stickelberger's theorem. *Finite Fields Appl.*, 14(3) :727–742, 2008.

[15] Philippe Langevin and Gregor Leander. On exponents with highly divisible fourier coefficients and conjectures of niho and dobbertin. In *Algebraic Geometry and its applications*, pages 410–418, 2008.

[16] Yves Aubry and Philippe Langevin. On the semiprimitivity of irreducible cyclic codes. In *Symposium on Algebraic Geometry and its Applications*, pages 284–293, Tahiti, 2008.

[17] Philippe Langevin, Gregor Leander, and Gary McGuire. A counterexample to a conjecture of Niho. *IEEE Trans. Inform. Theory*, 53(12) :4785–4786, 2007.

[18] Philippe Langevin, Patrice Rabizzoni, Pascal Véron, and Jean-Pierre Zanotti. On the number of bent functions with 8 variables. In *BFCA'06*, pages 125–135, Rouen, FRANCE, 2006.

[19] Yves Aubry and Philippe Langevin. On the weight of binary irreducible cyclic codes. In Springer, editor, *Workshop on Coding and Cryptography WCC'05*, volume 3969 of *Lecture Notes on Computer Sciences*, pages 46–54, Norway, 2006.

[20] Julien Bringer, Valérie Gillot, and Philippe Langevin. Exponential sums and Boolean functions. In *BFCA'05*, pages 177–185, 2005.

[21] Philippe Langevin and Pascal Véron. Non-linearity of power functions. *Designs codes and cryptography*, 37(1), 2005.

[22] Philippe Langevin and Jean-Pierre Zanotti. Finite groups and highly non-linear boolean functions. *Design, codes and cryptography*, 46(2) :131–146, 2005.

[23] Yves Aubry and Philippe Langevin. On the weight of binary irreducible cyclic codes. In *Book of Abstracts of the Workshop on Coding and Cryptography WCC'05*, pages 161–169, Bergen (Norway), 2005.

[24] Éric Brier and Philippe Langevin. The classification of boolean cubics of nine variables. In *2003 IEEE Information Theory Workshop*, La Sorbonne, Paris, France, 2003.

[25] Philippe Langevin and Jean-Pierre Zanotti. Around the counter example of Paterson and Wiedemann. In *Fq6*, pages 214–229. Finite Fields, 2002.

[26] Philippe Langevin and Patrick Solé. Gauss sums over quasi-Frobenius rings. In *Finite fields and applications (Augsburg, 1999)*, pages 329–340. Springer, Berlin, 2001.

[27] Philippe Langevin and Patrick Solé. Gauss sums over quasi-Frobenius rings. In *Fq5*, pages 329–341. Finite fields, 2001.

[28] Philippe Langevin and Patrick Solé. Z4 duadic codes. *Finite Fields and Their Applications*, 6 :309–326, 2000.

[29] Philippe Langevin. *Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes*. PhD thesis, Université de Toulon, January 1999.

[30] Philippe Langevin, Pascal Veron, and Jean-Pierre Zanotti. Fonction booléennes équilibrées (ii). Technical report, GRIM-SCSSI, 1998.

[31] Philippe Langevin and Patrick Solé. Kernels and defaults. In G. L. Mullen R. C. Mullin, editor, *Finite Fields : Theory, Applications and Algorithms*, volume 225 of *Contemporary Mathematics*, pages 77–87. AMS, 1998.

[32] Philippe Langevin. Sommes de gauss sur un anneau local. Technical Report 98–26, I3S, 1998.

[33] Philippe Langevin. Sur un théorème de Delsarte et McEliece. Technical Report 98–10, I3S, 1998.

[34] Philippe Langevin. Weight of abelian codes. *Designs, Codes and Cryptography*, 14(3) :239–247, 1998.

[35] Philippe Langevin. Calcul de certaines sommes de gauss. *Journal of Number Theory*, 62 :59–64, 1997.

[36] Xiang-Dong Hou and Philippe Langevin. Results on bent functions. *Journal of Combinatorial Theory (A)*, 80(2) :232–246, 1997.

[37] Philippe Langevin and Jean-Pierre Zanotti. Fonction booléennes équilibrées (i). Technical report, GRIM-SCSSI, 1996.

[38] Philippe Langevin. A new class of two weight codes. In *Finite Fields and Applications*, volume 233 of *London Mathematical Society Lecture Note Series*, pages 181–187. Cambridge, university press, 1996.

[39] Philippe Langevin and Jean-Pierre Zanotti. Linear codes with balanced weight distribution. *Applicable Algebra in Engineering, Communication and Computing*, 6(4-5) :299–307, 1995.

[40] Philippe Langevin. Regular section groups. *Finite Fields and their Applications*, 1(4) :405–412, 1995.

[41] Philippe Langevin. Some sequences with good autocorrelation properties. In *Finite Fields*, volume 168 of *Contemporary Mathematics*, pages 175–185, 1994.

[42] Philippe Langevin. Almost perfect sequences. *Applicable Algebra in Engineering, Communication and Computing*, 4 :95–102, 1993.

[43] Philippe Langevin. Construction of almost perfect sequences. In *Complexité, Codage, Compression Cryptographie*, volume xxx, pages 175–185, 1993.

[44] Philippe Langevin. On generalized bent functions. In *Eurocode 92*, volume 339 of *CISM Courses and Lectures*, pages 147–157, 1992.

[45] Philippe Langevin. *Rayon de Recouvrement des Codes de Reed-Muller affine*. PhD thesis, Université de Limoges, May 1992.

[46] Philippe Langevin. On the orphans and covering radius of the reed-muller codes. In *AAECC 9*, volume 539, pages 234–240, 1991.

[47] Philippe Langevin. The covering radius of $r(1,9)$ in $r(3,9)$. In *Eurocode 90*, volume 514 of *Lectures Notes in Computer Sciences*, pages 51–61. Springer-Verlag, 1990.

3. Encadrement

3.1. **mémoire de master.** Il s'agit des mémoires de master ou DEA sous ma responsabilité. Les travaux [1, 3, 4] ont donné lieu à une publication, le sujet [4] a été prolongé dans les postdocs [1, 2], alors que [5, 4] ont été des préliminaires importants à nos travaux de comptage des fonctions courbes.

Liste des Masters

[1] Serhii Dishko. Paramètres des codes quantiques. Master's thesis, master de mathématiques, université de Toulon, 2013. Ph. Langevin (Resp.) : General isometries of codes, YACC 2014.

[2] Banoun Anas. Construction de permutation APN. Master's thesis, master de mathématiques, université de Toulon, 2010.

[3] Eugene Zalinescu. Power functions. Master's thesis, DEA MDFI, Luminy, université d'Aix-Marseille, 2004. Analysis of Kasami-Welch Functions in Odd Dimension using Stickelberger's Theorem. Journal of Combinatorics and Number Theory 2 (1), 2011, 55 - 72.

[4] Eric Brier. The classification of boolean cubics of nine variables. Master's thesis, DEA MDFI, Luminy, université d'Aix-Marseille, 2002. 2003 IEEE Information Theory Workshop , La Sorbonne, Paris, France , 2003.

[5] Olivier Anglada. Etude des différentes orbites de $RM(3,9)/RM(2,9)$ sous l'action de $GL(2,9)$. Master's thesis, DEA informatique, Luminy, université d'Aix-Marseille., 2000.

[6] Stéphane Ballet. Autour du groupe d'automorphismes d'un code cyclique. Master's thesis, DEA informatique, Luminy, université d'Aix-Marseille., 1995.

[7] Jean-Pierre Zanotti. Applications booléennes et fonctions courbes. Master's thesis, maitrise de mathématique, Marseille., 1991.

3.2. **travaux de thèse.** Actuellement une thèse en cours (Serhii Dishko) qui a débuté en Décembre 2013. Les thèses plus anciennes ont été codirigées avec Jacques Wolfmann.

Liste des Thèses

[1] Serhii Dyshko. *paramètres métriques des codes quantiques*. PhD thesis, université de Toulon, 2013. Ph. Langevin (Dir.).

[2] Patrick Lacharme. *Générateur vraiment aléatoire dans un composant sécurisé*. PhD thesis, université de Toulon, 2008. Ph. Langevin (Dir.).

[3] Julien Bringer. *Non-linéarité des fonctions booléennes : applications des fonctions booléennes et des codes à la cryptographie*. PhD thesis, université de Toulon, 2007. Ph. Langevin (Dir.).

[4] Carine Boursier. *Corrélation de suites construites à partir de caractères multiplicatifs*. PhD thesis, université de Toulon, 1999. J. Wolfman (Dir.), Ph. Langevin (coDir.).

[5] Jean-Pierre Zanotti. *Codes à distribution de poids équilibrée*. PhD thesis, université de Toulon, 1998. direction Jacques Wolfmann.

[6] Oumar Mbodj. *Codes Cycliques et Sommes de Gauss*. PhD thesis, université de Toulon, 1997. J. Wolfmann (Dir.), Ph. Langevin (coDir.).

Jean-Pierre Zanotti est maître de conférence à l'université de Toulon. Oumar Mbodj est maître de conférence à l'université Gaston Berger au Sénégal. Carine Boursier est architecte sécurité Gemalto. Julien Bringer est expert en sécurité et cryptographe SAGEM sécurité et defense. Patrick Lacharme est chercheur au GREYC, maître de conférences à l' ensiCaen.

3.3. **jury de thèse.**

Liste des Jurys

[1] Kenza Guenda. *Habilitation universitaire*. PhD thesis, Université Houari Boumédiène, 2014. K. Betina, F. Z. Belkredim, D. Delhoul, M. Hernane, Ph. Langevin (exam.), F. Mokrane, M. Rezaoui.

[2] Stéphanie Dib. *Distribution de la nonlinéarité des fonctions booléennes*. PhD thesis, université d'Aix-Marseille, 2013. D. Augot, S. Ballet, G. Lachaud, P. Langevin (prés.), G. Leander, F. Rodier.

[3] Philippe Ravache. *Automorphismes projectifs et polynômes binaires irréductibles*. PhD thesis, université de Rouen, 2010. J.-F. Michon, C. Carlet, Ph. Langevin (rapp.), P. Solé, B. Vallée.

[4] Jean-Christophe Godin. *Problèmes de coloration et de choisissabilité dans les graphes*. PhD thesis, université de Toulon, 2009. Y. Aubry, Ph. Langevin (exam.), F. Maffray, A. Pêcher, O. Togni, Y. Vaxes.

[5] Pierre-Yvan Liardet. *Ingénierie cryptographique - Implantations sécurisées*. PhD thesis, Université de Montpellier, 2006. J.-C. Bajard, M. Girault, M. Joye, Ph. Langevin (rapp.), N. Smart.

[6] Stéphane Ballet. *Corps de fonctions algébriques et application à l'étude de la complexité bilinéaire de la multiplication dans les corps finis*. PhD thesis, (HDR) Université d'Aix-Marseille, 2006. I. Spharlinski, R. Rolland, G. Lachaud, R. Lercier, Ph. Langevin (exam.).

[7] Thomas Plantard. *Arithmétique modulaire pour la cryptographie*. PhD thesis, Université de Montpellier, 2005. J.-C. Bajard, D. Michelucci, R. Rolland, Ph. Langevin (exam.), M. Robert, L. Imbert.

3.4. **postdoc.** Il s'agit de jeunes docteurs que j'ai encadrés pour des séjours longs, financés par l'unité d'origine.

Liste des postdocs

[1] Elif Saygi. APN cubics in dimension 6. Tubitak University, 4 mois 2011. Ph. Langevin (Resp.).

[2] Zulfukar Saygi. APN cubics in dimension 6. Tubitak University, 4 mois 2011. Ph. Langevin (Resp.).

[3] Gregor Leander. counting bent functions. Ruhr-Universitat Bochum, 12 mois 2008. Ph. Langevin (Resp.).

3.5. **invitation.** Il s'agit de chercheurs invités pour une collaboration de 2 à 4 semaines, financés par l'Université de Toulon.

Liste des invitations

[1] Faruk Gologlu. Finite fields,exponential sums, 15 jours 2015.
[2] Jay Wood. Finite rings, 15 jours 2015.
[3] Daniel Katz. Weil sums. caltech, 15 jours 2014.
[4] Marcis Greferath. finite rings. Claude Shanon Institute, 1 mois 2011.
[5] Zulfukar Saygi. Apn mappings. Tubitak university, 1 mois 2011.
[6] Emrah CakCak. Helleseth conjecture. METU Ankara, 1 mois 2009.
[7] Xiang-Dong Hou. Partial spreads. South Florida University, 1 mois 2008.
[8] Gary McGuire. Finite fields. Claude Shanon Institute, 1 mois 2007.
[9] Gregor Leander. counting bent functions. Universität von Bochum, 1 mois 2006.
[10] Hans Dobbertin. counting bent functions. Universität von Bochum, 1 mois 2005.
[11] Jay Wood. code over rings. Univerty of Chicago, 1 mois 2000.
[12] Anna Bernasconi. Boolean functions. Universitià de Pisa, 1 semaine 1998.
[13] Xiang-Dong Hou. Bent functions. Wright State University, 1 mois 1997.

4. Diffusion

4.1. **communication.** Pour des raisons économiques et écologiques, je limite ma participation aux ateliers et conférences, moins de deux déplacements par an en moyenne, pour joindre les conférences :

- Arithmetic Geometry and Coding Theory,
- Boolean Function Cryptography and Application,
- Conference on Algebraic Informatics
- Finite Fields and Theirs Application,
- Workshop on Coding and Cryptography.
- Yet Another Conférence in Cryptology ;
- Journées C2 du GDR IM ;

Liste des conférences

[1] Philippe Langevin. Factorisation quantique. Toulon, France, Avril 2015. Journées Scientifiques de l'Université de Toulon. invité, vulgarisation.
[2] Philippe Langevin. Proof of a conjectured three-valued family of weil sums of binomials. Paris, France, Avril 2015. Worshop in Crypography and Coding Theory.
[3] Philippe Langevin. New open problems related to old conjectures by helleseth. Rosendal, Norway, September 2014. Boolean Functions and Applications. invited speaker.
[4] Yves Aubry and Philippe Langevin. On a conjecture of helleseth. Porquerolles, September 2013. CAI 2013.
[5] Philippe Langevin and Saygi Zülfukar. Apn mappings in dimension 6. Porquerolles, France, September 2012. Yet Another Cryptography Conference.

[6] Philippe Langevin. On helleseth conjecture. Marseille, june 2011. Arithmetic Geometry and Coding Theory.

[7] Philippe Langevin. Power permutation in dimension 32. Paris, September 2010. SETA 2010.

[8] Philippe Langevin. Gauss sums over finite rings. In *Ecole internationale : Codes over finite rings*, Ankara, Turquie, Aout 2008. CIMPA-METU. invited speaker.

[9] Philippe Langevin. Counting bent functions. Imath (Toulon), maaticah (Paris), 2008.

[10] Philippe Langevin and Gregor Leander. Classification of boolean quartic forms in eight variables. In *Boolean Functions in Cryptology anf Information Security*, Moscou, Russie, September 2007. NATO Advanced Study Institute. invited speaker.

[11] Philippe Langevin and Gregor Leander. On a conjecture of dobbertin. In *SAGA*, Papeete, France., May 2007. IML.

[12] Philippe Langevin and Gregor Leander. Testing main conjectures related to power functions. In *BFCA-07*, Paris, France., May 2007. LIAFA. invited speaker.

[13] Philippe Langevin, Patrice Rabizzoni, Pascal Véron, and Jean-Pierre Zanotti. On the number of bent functions with 8 variables. In *BFCA'06*, Rouen, 2006.

[14] Philippe Langevin. Correlation of sequences. In *Ecole internationale : suites pseudo-aléatoires*, Manille, Philippines, juillet 2005. CIMPA. invited speaker.

[15] Philippe Langevin and Gregor Leander. Monomial bent functions. Marseille, France., September 2005. Arithmetic Geometry and Coding Theory.

[16] Julien Bringer, Valérie Gillot, and Philippe Langevin. Exponential sums and Boolean functions. Rouen, 2005. Boolean Functions and Applications.

[17] Yves Aubry and Philippe Langevin. Cyclic codes with few different weights. In *AGCT-10*, Marseille, France., September 2005. Arithmetic Geometry and Coding Theory.

[18] Yves Aubry and Philippe Langevin. On the weight of irreducible cyclic codes. Bergen, Norway., March 2005. Workshop on Coding Theory and Cryptography.

[19] Eric Brier and Philippe Langevin. The classification of boolean cubics of nine variables. "La Sorbonne", Paris, France, 2003. 2003 IEEE Information Theory Workshop.

[20] Philippe Langevin. Classification of boolean cubics of 9 variables. In *Arithmetique et Combinatoire*, Luminy, France, 2002.

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

[22] Philippe Langevin. Nonlinearity of power functions. In *yacc-02*, Porquerolles, France, 2002. GRIM.

[23] Philippe Langevin. About the counter-example of Patterson et Wiedeman. In *Fq6*, Oaxaca, Mexico., june 2001. Finite Fields and Applications.

[24] Philippe Langevin. Non-linearity of power functions. In *AGCT-8*, Luminy, France, 2001. IML. Conférencier invité.

[25] Philippe Langevin and Patrick Solé. Gauss sums over quasi-frobenius rings. In *Fq5*, Augsburg, Allemagne, 2000. Finite Fields and Applications.

[26] Philippe Langevin. Gauss sums over quasi-frobenius rings. Augsburg, August 2-16 1999, Germany, 1999. FQ5.

[27] Philippe Langevin. On generalized bent functions. In *Designs, Sequences and their correlations*, BadWindsheim, aout 1998, 1998.

[28] Philippe Langevin. Somme de gauss sur un anneau de local. Lab. GECT, 1998.

[29] Philippe Langevin. Kernel and default. In *Fourth International Conference on Finite Fields and Applications*, Waterloo, Canada, August, 1997. FQ4.

4.2. **séjour de recherche.**

ITSC at Bochum	2 semaines	(2006)
Université Gaston Berger	1 mois	(2001)
Université Gaston Berger	1 mois	(2000)
CNRS, I3S	2 ans	(1998, 1999)
Wrigth State University	2 semaines	(1997)

4.3. **arbitrage.** Je rapporte régulièrement sur les travaux soumis aux revues de mon domaine. Je rapporte sporadiquement sur les projets de recherche soumis à des organismes français (ECOsud) ou étrangers (NSA).

4.4. **animation.** J'organise le séminaire de recherche de l'équipe Informatique et Algèbre Appliquée de l'IMATH. Je contribue à l'organisation des rencontres "calcul" des laboratoires LSIS, IMATH et MIO de l'université de Toulon.

4.5. **Organisation.** Je suis co-organisateur, co-chair, des éditions de la conférence internationale *Yet Another Conference in Cryptology*, un évènement bisannuel sur les thématiques de recherche de l'équipe IAA du laboratoire IMATH.

Je suis dans le comité des programmes des conférences :

– Yet Another Conference in Cryptology
GRIM, IMATH.
Porquerolles, 2002, 2004, 2006, 2008, 2010, 2012, 2014.
. . . . . http ://yacc.univ-tln.fr

– Journées Codage et Cryptographie 2015.
conférence du groupe C2 du GDR-IM.
La londe, Octobre 2015.
. . . . . http ://imath.univ-tln.fr/C2

– ICCC 2015
International Conference on Coding and Cryptography",
USTHB, Alger, 2-5 Novembre 2015.
. . . . . http ://www.latn.usthb.dz

4.6. **vulgarisation.** J'utilise mon site web pour diffuser mes codes, reflexions, brouillons, notes historiques, cours, projets, etc. . . Plus de 6000 fichiers sont disponibles sur ce site dont le pagerank vaut 4. Certaines de mes notes de vulgarisation sont assez populaires :

– Emanuel Lasker, arithméticien champion du monde ;
Une note qui s'adresse au monde échiquéen dans laquelle je précise la nature de la contribution mathématique du champion de monde.

http ://langevin.univ-tln.fr/notes/Lasker/Lasker.html

– Le testament d'Évariste Galois.
  Une note de plus sur les galoiseries. Elle est bookemarquée dans les signets de la Bibliothèque Nationale de France.

http ://langevin.univ-tln.fr/notes/Galois/Galois.html

4.7. **projet numérique.** J'utilise mon site web pour décrire et diffuser les données résultantes de mes projets numériques.
. . . . . http ://langevin.univ-tln.fr/project

5. Responsabilité scientifique

5.1. **comité de selection.**
– 2012 Président comité de sélection, recrutement PR-27 Toulon.
– 2011 Président comité de sélection, recrutement PR-27 Toulon.
– 2010 Président comité de sélection, recrutement MC-27 Toulon.
– 200 ? Membre élu commission de spécialite section 27.

5.2. **responsabilité.**
– 2012- directeur adjoint de l'institut de mathématique de Toulon.
– 2008-12 responsable de l'équipe (IAA) Informatique et Algèbre Appliquée du laboratoire IMATH.
– 2004-2011 correspondant du site Toulonnais pour le groupe C2 du GDR-IM.
– 2004-2008 direction du Groupe de Recherche en Informatique et Mathématique.
. . . . . http ://imath.univ-tln.fr

6. Enseignement

Depuis que je suis enseignant-chercheur, je me suis investis dans plusieurs enseignements à chaque fois, il fût question de construire les cours, planches de travaux-dirigés et les sujets de travaux-pratiques. Par le passé, j'ai enseigné : la théorie des langages (L3 info), l'algorithmique et la complexité (M1 info), la calculabilté et la décidabilité (M1 info), la théorie des codes correcteurs (M1 info), la cryptanalyse et la cryptographie (M2 info), la théorie de l'information (M1 info), les structures algébriques finies (L2 info), quelques applications de l'arithmétique et la théorie de Galois aux télécommunications numériques (M2 math). Ces dernières années, mon activité pédagogique porte sur l'algorithmique, la programmation système et réseau, la compilation et l'encadrement de stagiaires du master de mathématiques.

6.1. **stage.**

TAB. 1. activité pédagogique récente dans les départements d'informatique et de mathématiques.

année	intitulé	niveau	section
2008-2012	langage C avancé	L1	info
2008-2013	preuve et analyse des algorithme	L2,3	info
2012-2013	unix et programmation shell	L3	info
2008-2013	langage et compilation	L3	info
2008-2011	réseau	M1	info
2012-2013	arithmétique en langage C	M1	info
2012-2013	application des corps finis	M2	math

—

[1] Jonathan Ben-Naim. Distribution du calcul d'énumérateur de poids avec pvm. Master's thesis, DEUG, sujet libre, 2001.

[2] Stéphane Renouf. Les corps non-commutatifs. Master's thesis, 1997.

[3] Camar Eddine. Nombre de classes et théorème de fermat. Master's thesis, TER maitrise de mathématique, 1996.

[4] Karine Adamczewki. La loi de réciprocité quadratique de gauss. Master's thesis, TER maitrise de mathématique, 1995.

[5] Yves Gaudumet. Algorithme de factorisation de berlekamp. Master's thesis, TER maitrise de mathématique, 1994.

[6] Jean-Pierre Zanotti. Applications booléennes et fonctions courbes. Master's thesis, TER maitrise de mathématique, 1991.

DÉPARTEMENT D'INFORMATIQUE, INSTITUT DE MATHÉMATIQUE DE TOULON, UNIVERSITÉ DE TOULON, U.F.R. DES SCIENCES ET TECHNIQUES, BÂTIMENT U, AVENUE DE L'UNIVERSITÉ, B.P. 20132 83957 LA GARDE CEDEX.

E-mail address: langevin@univ-tln.fr

URL: http ://langevin.univ-tln.fr