Curriculum vitæ
et synthèse des travaux de recherche

Jean-Marie Le Bars
Université de Caen Normandie
UFR Sciences

Sommaire

Chapitre 1

Synthèse de la carrière

Etat civil

Jean-Marie Le Bars
Maître de conférences
Section CNU : 27
Date de naissance : 2 décembre 1966
Situation familiale : marié, 4 enfants
Établissement : Université de Caen Normandie
Laboratoire GREYC (UMR 6072)
Équipe de recherche : Monétique & Biométrie
Adresse électronique : jean-marie.lebars@unicaen.fr
page Web : https ://www.greyc.fr/fr/users/lebarsj
Adresse personnelle : 7 rue des loisirs 14610 Epron

Expérience professionnelle

depuis 1999 - maître de conférences à l'Université de Caen Normandie
2003-2004 - délégation de deux ans au LIPN
1998 - poste d'ATER à temps complet à l'Université de Caen Normandie, enseignant au CNAM
1994 - 1997 - Vacataire en informatique et en mathématiques à l'Université de Caen Normandie

Parcours universitaire

juin 2016 - Habilitation à diriger les recherches intitulée « Quelques études de l'aléatoire en informatique »Rapporteurs : P. Duchon, J-Y Marion, J-P Tillich
Jury : P. Duchon, C. Charrier, E. Grandjean,J-Y Marion, C. Rosenberger, J-P Tillich
janvier 1998 - Thèse de doctorat de l'Université de Caen Normandie intitulée « Probabilités asymptotiques et pouvoir d'expression des fragments de la logique du second ordre ».
Rapporteurs : P. G. Kolaitis, J. Lynch, M. de Rougemont
Jury : S. Abitboule, P. Dehornoy, W. Fernandez de la Vega, E. Grandjean (directeur), J. Stern, P. Toffin, B. Vallée.
1994 - DEA d'algorithmique et d'arithmétique à l'Université de Caen Normandie
1993 - Maîtrise de Mathématiques à l'Université de Caen Normandie

Enseignements

Algorithmique et programmation
Mathématiques discrètes
Programmation orientée objet
Probabilités et statistiques
Génération et tests aléatoires

Algorithmes probabilistes
Outils algorithmiques pour la cryptographie

Responsabilités actuelles

Directeur-adjoint du département d'informatique (2011-2015)
Responsable des formations d'informatique (depuis 2011)
Directeur des études de la licence d'informatique (depuis 2011)
Porteur des maquettes de la licence d'informatique (maquette 2012-2017 et 2017-2022)
Membre élu du conseil de l'UFR (depuis 2011)

Recherche

Études algorithmiques et combinatoires des structures aléatoires
Outils algorithmiques pour la sécurité (cryptographie, biométrie, tatouage)
Mise en place et étude de la sécurité de systèmes d'authentification

Publications

4 revues internationales
13 conférences internationales avec actes et comité de lecture,
1 conférence nationale avec comité de lecture.

Rayonnement

Co-organisation de quatre conférences, deux conférences internationales (AofA2001, Number, sequences, Lattices 2010) et deux conférences nationales (Aléa2005, école Jeunes chercheurs en algorithmique et calcul formel 2000)
Comité de lecture de multiples conférences internationales et revues
Expertise de projets (1 ANR, 1 ACI)

Encadrement de thèses

Une thèse soutenue en 2010 (encadrement à 50%), une thèse soutenue en 2015 (encadrement à 33%)
Une thèse en cours (encadrement à 33%)

Chapitre 2

Activités pédagogiques

2.1 Responsabilités pédagogiques

Mise en place de la licence d'informatique
Depuis que je suis en poste à l'Université de Caen Normandie, je me suis toujours activement impliqué dans le suivi de nos formations en informatique, en particulier pour la licence d'informatique. La réforme LMD nous a permis d'élaborer pour la première fois un parcours informatique sur les trois premières années de la licence, auparavant la licence d'informatique se faisait en une année après un DEUG de mathématiques ou de physique-chimie (SM). J'ai participé en 2003-2004 avec Patrice Enjalbert, alors président de la commission pédagogique, à ce vaste chantier où toute notre formation a dû être remise à plat. J'ai piloté en 2010 la maquette de la mention informatique de la licence sciences et technologies (regroupant toutes les mentions de l'UFR sciences) pour son renouvellement pour la période 2012-2017. Il faut noter que la mention informatique a été la seule sur toutes les licences de l'Université de Caen Normandie à obtenir une évaluation A+ par l'AERES en partie grâce à un bon compromis entre une finalité scientifique généraliste et professionnelle. J'ai mis en place pour la prochaine maquette 2017-2022 un comité de pilotage. L'effectif total des trois années de licence a considérablement augmenté, il est passé de 200 en 2012-2013 à 350 en 2014-2015, ce qui complexifie considérablement son organisation en partie pour le suivi des enseignements et le suivi des étudiants.

Promotion des formations du département d'informatique
J'ai animé à de nombreuses reprises des conférences pour présenter nos formations aux lycéens (journées du lycéen, salon de l'étudiant). J'interviens également auprès des étudiants de L1 et L2 pour leur présenter les différentes formations en informatique, licences professionnelles et master. J'ai participé à la rédaction de flyers présentant les formations du département d'informatique. Je participe depuis 5 ans à une conférence sur les métiers de l'informatique au salon de l'étudiant de Caen.

Méthodes pédagogiques
Je m'intéresse fortement à la mise en place de nouvelles méthodes pédagogiques. J'ai introduit pour la maquette 2012-2017 de la licence d'informatique un encadrement de projet sur les deux semestres du L2 appelé TPA (Travaux Personnels Approfondis) qui permet un travail par groupe de quatre à six étudiants suivis par un enseignant tout au long de l'année. J'expérimente la pédagogie inversée dans la valeur de tests aléatoires en M1, les étudiants n'ont que des TP et les notions de cours sont incluses dans les énoncés des TP et expliquées à la demande en fonction des besoins des étudiants pendant la réalisation des TP.

2.2 Présentation synthétique des enseignements

Mes enseignements de prédilection portent sur l'informatique mathématique, l'algorithmique et l'aléatoire. Ces dernières années, j'ai enseigné les matières suivantes :

- Initiation à la programmation en python L1
- Mathématiques pour l'informatique L2
- Structures de données et algorithmique L2
- Programmation orientée objet L2
- Mathématiques discrètes (combinatoire analytique et analyse d'algorithmes) L3
- Probabilités et statistiques pour l'informatique M1
- Tests aléatoires (modélisation aléatoire, protocoles de tests) M1
- Structures aléatoires (graphes aléatoires, fonctions booléennes pour la cryptographie) M2
- Algorithmes probabilistes M2

Je suis bien sûr disposé à assurer d'autres types d'enseignements selon les besoins du département d'informatique. J'essaierai, si possible, de toujours enseigner du L1 jusqu'au M2, car cela permet une meilleure vision verticale de nos diplômes.

Je compte de plus m'investir davantage sur les projets des étudiants, car c'est à mon avis un point crucial pour améliorer la qualité de nos formations. En effet, cela permet d'une part aux étudiants de mettre en application efficacement les concepts vus en cours et cela produit d'autre part un lien naturel entre nos activités de recherche et les compétences que doivent acquérir les étudiants lors du master. J'ai ainsi encadré pendant l'année 2014-2015 quatre projets en M1 et M2 du master e-SECURE sur des thématiques liées à ma nouvelle équipe de recherche, trois projets en biométrie et un en authentification.

Activités pédagogiques à l'Université de Caen Normandie avant d'être maître de conférence

Diplôme	Enseignement	CM	TD	TP	Année
DEUG A 1ère année	Mathématiques		48		1993-1994
DEUG A 2ème année	Mathématiques		48		1993-1994
DEUG B 2ème année	Introduction à la programmation		24	24	1996-1998
CNAM	Programmation ADA		50		1998-1999
DEUG A 2ème année	Introduction au C++		15	15	1998-1999
DEUG LEA 2ème année	Environnement informatique		40	40	1998-1999
Licence LEA	Introduction au C		20	20	1998-1999

Activités pédagogiques à l'Université de Caen Normandie avant le LMD

Diplôme	Enseignement	CM	TD	TP	Année
DEUG A 2ème année	Introduction au C++		15	15	1999-2002
Licence d'informatique	Mathématiques pour l'informatique	25	25		1999-2003
DEUG SM	Algorithmique et programmation en pascal	19,5	13	14	1999-2003
DEUG A 2ème année	Programmation orientée en java		30	30	1999-2003
M1 neurosciences	Bases de données	12	15	15	1999-2003
Licence pro webmestre	Introduction à la sécurité	6	6		1999-2003
DESS NAPI	Algorithmique en java	6	4	11	1999-2003
DESS RADI	Transactions sécurisées	9	11		1999-2003
DESS RADI	Graphe du web	3	3		2000-2003

Activités pédagogiques à l'Université de Caen Normandie après le LMD

Diplôme	Enseignement	CM	TD	TP	Année
L1 Info	Introduction à la programmation		19,5	19,5	2006-2012
L2 Info	Mathématiques pour l'informatique	20	30		2005-2011
L2 Info	Structures de données et algorithmique		26	13	2012-2015
L2 Info	Programmation orientée objet		19,5	19,5	2013-2015
L3 Info	Mathématiques discrètes	20	30		2006-2014
M1 Info	Probabilités et statistiques	10	10		2011-2015
M1 Info	Tests et modèles aléatoires	20	20		2011-2015
M2 AMI	Structures aléatoires et analyse d'algorithmes	8			2006-2012
M2 e-SECURE	Outils algorithmiques pour la cryptographie	10			2013-2015

Chapitre 3

Activités d'administration

3.1 Activités liées à l'enseignement

Commission pédagogique

2000-2010 Vice-président de la commission pédagogique
2000-2005 Coordinateur des enseignements d'informatique en DEUG MIAS et SM
2003-2005 Participation à la mise en place de la licence d'informatique lors du passage au LMD

Responsabilités au sein du département d'informatique

- Directeur adjoint du département d'informatique
- Responsable des formations (remplace la commission pédagogique)
- Responsable de la licence d'informatique (directeur des études)
- Porteur des maquettes de la licence d'informatique 2012-2017 et 2017-2022

Conseil de l'UFR
Je suis fortement impliqué dans l'animation pédagogique à l'UFR sciences. J'ai été élu au conseil de l'UFR en mars 2011 et réélu en mai 2015. Je participe à tous les conseils (environ un par mois). J'ai participé à une réunion préparatoire à la fusion entre l'UFR de Sciences et l'IBFA avec des représentants des deux composantes. J'ai aussi participé à des discussions avec la direction du département de mathématiques car nos deux départements doivent se regrouper.

3.2 Activités liées à la recherche

Direction de thèses
co-encadrement à 50 % avec Jacques Madelaine de la thèse de Cyril Bazin intitulée ≪Tatouage de données géographiques et généralisation aux données devant préserver des contraintes≫, soutenue en janvier 2010. Après avoir occupé un postdoc à l'Université de Caen Normandie dans le framework Sydony, il travaille depuis 2014 à DATEXIM, une start-up dans le traitement, l'analyse et la visualisation d'images médicales où il dirige l'équipe R&D.

Depuis mon arrivée début 2014 dans l'équipe Monétique et Biométrie, je co-encadre deux thèses en Biométrie avec Christophe Rosenberger et Christophe Charrier comme codirecteurs.

Je co-encadre à 33% la thèse de Benoit Vibert intitulée *Evaluation d'algorithmes de comparaison embarquée sur carte à puce (Match-On-Card)*. La soutenance est prévue fin 2016.

J'ai co-encadré à 33% la thèse de Zhigang Yao intitulée *Evaluation de la qualité des empreintes digitales*. Thèse soutenue en juillet 2015.

Collaborations nationales

2009-2013 membre de l'ANR programme blanc Boole, responsable du site de Caen
2004-2008 membre de l'ACI sécurité Tadorne, responsable du site de Caen
2002-2004 membre de l'AS, Nouveaux modèles de calcul
2001-2004 membre de l'ACI Cryptologie

Collaboration internationales

2013-2014 DYNALCO, projet de collaboration STIC-AmSud avec l'Argentine et l'Uruguay
2009-2012 projet de coopération ECOS-sud avec L'Uruguay

Groupes de recherche

- membre du GDR IM (Informatique mathématique)
- membre du groupe de travail Aléa du GDR IM
- membre du groupe de travail C2 (Codage et Cryptographie) du GDR IM
- membre du groupe international AofA (Analysis of Algorithms)

Evaluation de la recherche

- expertise d'une ANR programme blanc en 2012
- expertise d'une ACI en 2005
- rédaction de plus d'une trentaine de rapports pour des conférences et des journaux internationaux

Organisation de conférences

- membre du comité d'organisation de la conférence Numbers, Sequences, Lattices : Dynamical Analysis of Algorithms à Caen en juin 2010.
- co-organisateur des journées Aléa en 2005 au CIRM.
- membre du comité d'organisation des rencontres internationales d'analyse d'algorithmes AOFA2001 Tatihou, France
- membre du comité d'organisation de l'école Jeunes chercheurs en algorithmique et calcul formel à Caen (2000)

Organisation de séminaire

2001-2003 Responsable du séminaire hebdomadaire Algorithmique du GREYC.

Jurys de thèse

janvier 2010 membre du jury de la thèse de Cyril Bazin (co-direction à 50%)
juillet 2015 membre du jury de la thèse de Zhigang Yao (co-encadrement à 25%)

Délégation CNRS [septembre 2003- août 2005]

J'ai obtenu deux années de délégation CNRS au LIPN. Cela m'a permis de collaborer avec plusieurs membres du LIPN et d'élargir mes domaines de compétences en algorithmique et en combinatoire.

Implication dans le laboratoire

2007-2011 élu au conseil du laboratoire du GREYC.
2005-2008 membre extérieur de la commission de spécialistes du LIPN, université Paris XIII.
2004-2008 membre de la commission de spécialistes du GREYC.

Chapitre 4

Activités de recherche

4.1 Thèmes de recherche

Mes thèmes de recherche –en apparence très dissemblables– révèlent les différents aspects de l'étude de l'aléatoire. Pour simplifier, on peut considérer les aspects suivants :

Thème 1 On modélise les structures réelles et on peut s'intéresser aux propriétés des structures générées par ce modèle, on peut ainsi conduire des études mathématiques lorsque la taille des structures augmente (calculs asymptotiques).

Thème 2 On extrait de l'aléa de données réelles en effectuant des tests statistiques sur celles-ci.

Thème 3 On cherche à produire efficacement des données aléatoires (par exemple, en construisant des générateurs aléatoires de structures).

4.2 Domaines de recherche

Depuis que j'ai commencé ma thèse en 1994, je m'intéresse aux propriétés des structures aléatoires discrètes pour des problèmes issus de domaines très différents :

$d1$ logique (théorie des modèles finis)

$d2$ phénomènes de seuil et transitions de phase

$d3$ analyse d'algorithmes

$d4$ tatouage de données géographiques

$d5$ fonctions booléennes pour la cryptographie

$d6$ étude des systèmes d'authentification à base de biométrie et de cryptographie

Toutes ces études sauf la dernière ont été effectuées dans la même équipe, l'équipe Algorithmique du GREYC, qui est devenue l'équipe AMACC en 2010. La dernière étude s'effectue dans l'équipe Monétique et Biométrie que j'ai intégrée début 2014. Je m'intéresse depuis aux aspects aléatoires de structures discrètes intervenant dans les domaines de la Biométrie et de la Confiance. Ce changement d'équipe me permet d'une part d'être confronté à l'expérimentation (évaluation des protocoles proposés) alors que cet aspect de la recherche était très peu considéré dans ma précédente équipe et d'avoir de meilleures opportunités d'encadrements de thèse. Depuis ce changement d'équipe, je co-encadre deux thèses en Biométrie sur l'étude des minuties issues d'empreintes digitales.

4.3 Études réalisées

Noyaux dans les graphes (thème 1, d1, d2, d3)
Le noyau d'un graphe orienté est un sous-ensemble de sommets dominant et stable. L'existence d'un noyau dans un graphe est une propriété NP-complète qui apparaît naturellement dans des domaines tels que la théorie des jeux ou l'intelligence artificielle. Mon résultat principal de thèse a été de montrer que cette propriété jouait un rôle central de contre-exemple aux lois 0-1 en logique du second ordre en permettant de résoudre plusieurs problèmes ouverts. Il est apparu comme un résultat très marquant du domaine et j'ai obtenu deux distinctions en 1998, un prix national –un accessit du prix SPECIF 98– et un prix international– le Kleene award, prix du meilleur papier étudiant de la plus grande conférence de logique en informatique (LICS, conférence classée CORE A*). J'ai depuis poursuivi mes recherches sur cette propriété dans d'autres domaines d'application, en intelligence artificielle (lois 0-1 en logique modale), sur les phénomènes de seuil et en analyse d'algorithmes (calcul de probabilités asymptotiques avec la méthode des moments ou l'utilisation de séries génératrices). Mes derniers travaux dans ce domaine portent sur dans les graphes creux (graphes ayant un nombre linéaire d'arcs par rapport au nombre de sommets). J'ai obtenu avec Marco Illengo la probabilité d'avoir un noyau dans ces graphes.

Tatouage de données géographiques (thème 2, d4)
J'ai codirigé à 50% avec Jacques Madelaine la thèse de Cyril Bazin qui a soutenu sa thèse en janvier 2010. La méthode de tatouage consiste à découper un document géographique en sites en utilisant une triangulation de Delaunay et à insérer une marque en modifiant de l'aléatoire contenu dans ces sites [13]. Cette méthode a ensuite été généralisée pour d'autres types de documents tels que les bases de données relationnelles [12].

Fonctions booléennes pour la cryptographie (thème 3, d3,d5)
Je travaille depuis 2006 avec Alfredo Viola sur l'énumération et la génération aléatoire de fonctions booléennes selon des critères cruciaux pour la cryptographie symétrique. Notre approche est à la fois combinatoire et algorithmique, elle allie l'analyse d'algorithmes (série génératrices, méthode récursive), la théorie de l'information (codage énumératif) et des méthodes fines de programmation pour limiter l'explosion combinatoire. Cela nous a permis avec un étudiant uruguayen Nicolas Carrasco de compter le nombre de fonctions 1-résilientes (fonctions équilibrées et sans corrélation d'ordre 1) jusqu'à 8 variables (plus de 10^{67}) et de construire un générateur aléatoire pour les générer avec la distribution uniforme. Ces études ont donnée lieu à quatre publications, deux en conférence internationale et deux dans les journaux *Transactions on Information Theory*, rang A* à CORE, et *Theoretical Computer Science*, rang A à Core.

Nos projets futurs concernent l'énumération des fonctions sans corrélation d'ordre quelconque de petit poids de Hamming et les liens avec un domaine de la combinatoire (combinatorial designs).

Fonctions coïncidentes (voir projet ANR Boole)
Je travaille depuis 2012 avec Hayat Cheballah et Morgan Barbier sur la construction et l'énumération des fonctions coïncidentes. Nous allons soumettre une partie des résultats obtenus dans le journal *Cryptography and Communication* en juillet 2015.

Tatouage d'images et biométrie révocable
En collaboration avec Christophe Rosenberger et Morgan Barbier, je travaille sur l'utilisation de méthodes de biométrie révocable (le biohashing permet cette révocabilité) pour prouver l'identité du propriétaire d'un document numérique. Notre article *Image Watermaking With Biometric Data For Copyright Protection* accepté au workshop MFSec (Multimedia Forensics and Security), sélectionné par le comité de programme de la conférence internationale *Availa-*

bility, Reliability and Security (ARES), qui se déroulera à Toulouse fin août 2015. Une version étendue sera soumise au journal *Computers & Security*.

Répartition des minuties d'une empreinte digitale (thème 2 et 3, d6)
Je travaille sur la modélisation aléatoire des templates de minuties d'empreintes digitales. C'est un sujet en lien avec les deux thèses que je co-encadre (sur la sélection de minuties et sur la qualité des templates). Il s'agit de déterminer les caractéristiques qui sont communes à tous les templates et celles qui changent d'une personnes à une autre. Une des pistes explorées est d'effectuer une triangulation de Delaunay et de comparer ces triangulations.

4.4 Encadrement en recherche

L'encadrement d'étudiants de master, de doctorants ou de postdoctorants est une des activités les plus intéressantes d'un enseignant-chercheur. Plus que les résultats de recherches auxquelles je peux ainsi contribuer, c'est la formation d'un chercheur qui me semble le plus passionnant. Par exemple, pour un doctorant, il s'agit non pas de le diriger pour qu'il fasse le travail que l'on aurait fait, mais lui donner les moyens pour qu'il puisse réaliser la thèse correspondant à ses capacités et ses envies, tout en vérifiant bien sûr que les objectifs du sujet de thèse soient atteints.

4.5 Encadrements de thèse

Thèse de Cyril Bazin, soutenue en 2010
Ma première expérience avec Cyril Bazin fut à ce niveau particulièrement satisfaisante. Je participais à une ACI sécurité intitulée *Tadorne* sur le tatouage de données structurées notamment sur des données géographiques vectorielles. Ce projet impliqué les laboratoires *Cedric* du Cnam-Paris, le *COGIT* de l'IGN, le *Lamsade* de l'univerité Paris-Dauphine et le *GREYC*. C'était un projet très innovant, car contrairement aux images et aux données vidéos, peu d'études avaient été faites pour le tatouage de données structurées. Avec Jacques Madelaine, maître de conférences au GREYC, nous avons eu l'idée d'un sujet sur un tatouage aveugle (sans connaissance du document original) et robuste à des transformations naturelles comme la rotation et le découpage. J'ai défendu ce sujet devant la commission de la recherche du conseil régional, il a été classé premier sur l'ensemble des thèses proposées toutes disciplines confondues. C. Bazin a obtenu dès sa première année des résultats très intéressants en utilisant la triangulation de Delaunay sur des documents géographiques et en introduisant un biais statistique sur des caractéristiques de ces triangles. Il a ensuite eu plus de difficultés à formaliser son approche et à s'abstraire du type de données considéré afin d'avoir des résultats plus génériques. C'est sur ces deux aspects –la formalisation et la généralisation de son travail– que mon apport a été le plus important.

Thèse de Zhigang Yao, soutenue 21 juillet 2015
Depuis mon arrivée dans l'équipe Monétique et Biométrie en janvier 2014, je co-encadre à hauteur de 25% la thèse de Zhigang YAO avec C. Rosenberger et C. Charrier. Nous travaillons sur l'évaluation de mesures de la qualité des empreintes digitales. Cette évaluation s'effectue sur des templates (ensemble de minuties) sans avoir accès à la donnée biométrique originale, cela nécessite une notion de qualité différente de celle liée à la perception humaine. La mesure de qualité doit aussi être robuste, le plus possible invariante par rapport aux logiciels utilisés pour les expérimentations (enrôlement, matching). Certaines méthodes utilisent la triangulation de Delaunay, ce qui permet de faire le lien avec la thèse de Cyril Bazin où la notion de préservation de qualité était aussi un aspect très important. Depuis que je co-encadre cette thèse, j'ai cosigné plusieurs articles, j'ai également fait un exposé à la conférence ISBA à Hong Kong en mars 2015 pour présenter un de ses articles. Je participerai au jury de sa thèse.

Thèse de Benoit Vibert
Je co-encadre aussi depuis mon arrivée dans ma nouvelle équipe de recherche la thèse de Benoit Vibert avec C. Rosenberger et C. Charrier. Il travaille sur la sélection de minuties pour construire un template de taille fixée, limitation nécessaire par exemple pour MOC (Match On Card). Il s'intéresse également aux attaques. Enfin, il implémente les nouvelles fonctionnalités dérivées de son travail dans la plate-forme Evabio développée dans l'équipe. La thèse devrait être soutenue avant décembre 2016.

4.6 Encadrement de postdoctorants

Le terme postdoctorant signifie ici une personne ayant soutenue sa thèse et qui n'a pas encore obtenu de position permanente, typiquement une personne ayant un poste d'ATER ou ayant un contrat postdoctoral. Il ne s'agit pas de fournir un encadrement comme pour un étudiant en master ou en thèse, mais plutôt de faire partager mon expérience en recherche, communiquer mes méthodes de travail et les former à mes domaines de recherche. Ces expériences sont très enrichissantes, j'ai contribué non pas à initier à la recherche comme pour un doctorant, mais à compléter et à renforcer une formation de chercheur pour des docteurs ayant travailler dans d'autres domaines plus ou moins connexes.

Collaboration franco-uruguayéenne
Depuis 2009, dans le cadre d'un projet ECOS franco-uruguayen, nous co-encadrons, Alfredo Viola et moi, un étudiant uruguayen Nicolas Carrasco. Celui-ci a exposé nos travaux sur la génération aléatoire à la conférence internationale ITW au Brésil en octobre 2011. Carrasco est venu fin 2011 un mois à l'université de Caen pour travailler sur ces sujets. Nous avons publié tous les trois en 2013 un article dans le journal TCS (Theoretical Computer Science).

Pendant l'année 2014-2015, Alfredo Viola a proposé un projet annuel de deux étudiants, Sebastián Foncesa et Maria Cecilia Garcia pour programmer des méthodes d'énumérations de fonctions sans corrélation de petit poids de Hamming en implémentant des algorithmes que j'ai définis.

Projets et stages de master
J'ai déjà encadré de nombreux projets et stages de master. Actuellement, les projets annuels en M1 et en M2 sont particulièrement bien adaptés pour initier les étudiants à mes activités de recherche. J'ai cette année 2014-2015 encadré quatre projets en M1 et M2 sur des sujets intéressant mon équipe de recherche et pour deux d'entre-eux –sur les triangulations de Delaunay pour les empreintes digitales– les résultats vont être utilisés pour les travaux de thèse de Benoit Vibert.

4.7 Publications

4.7.1 Choix des publications

Les habitudes de publications sont vraiment très différentes d'une discipline à une autre et même pour une même discipline, d'un domaine à un autre. Je sais, par exemple, qu'en mathématiques, les conférences ne jouent pas un rôle très important en terme de diffusion des résultats. En informatique, dans certains domaines (comme la cryptographie) les meilleurs publications se font dans des conférences. J'ai choisi la conférence LICS (Logic In Computer Science) pour mes deux meilleurs résultats en logique (théorie des modèles finis) ([16] et [17]). La conférence est de rang A* dans CORE (Computing Research and Education Association of Australasia) le site de classification des publications en informatique le plus réputé. Il n'existe pas de revue en logique plus réputée et avec une audience plus large. Grâce à ces publications, les meilleurs chercheurs du domaine comme Vardi, Gurevich, Kolaitis ont pu découvrir mes

résultats et me signifier qu'ils appréciaient mon travail. C'est pourquoi j'estime que ces deux publications ont la même valeur que des revues de rang A*.

En revanche, d'autres conférences comme ISIT ([14]) et ITW ([11]) ont également une très large audience, mais le format (6 pages) est insuffisant pour développer les parties techniques. C'est pourquoi nous avons dans les deux cas publié une version étendue dans les revues Transaction in Information Theory ([4], classée rang A* par CORE) et Theoretical Computer Science ([2], classé rang A par CORE)

4.7.2 Sélection de cinq publications significatives

1. J-M. Le Bars. Counterexamples of the 0-1 law for fragments of existential second-order logic : an overview. Bulletin of Symbolic Logic, 9 :67–82, 2000. impact facteur 0,917

   Il s'agit d'un survey destiné à une large communauté en logique qui reprend les contre-exemples de lois 0-1 en logique existentielle du second-ordre, en particulier mes résultats principaux de thèse. Ceux-ci ont permis de résoudre les derniers problèmes ouverts sur le sujet et également de fournir un unique contre-exemple unifiant tous les résultats sur ce sujet. Le journal *Bulletin of Symbolic Logic* est dédié aux articles de haut niveau dont le sujet est susceptible d'intéresser un large public en logique mathématique, en logique philosophique, en histoire de la logique et en philosophie des mathématiques. Il fait partie du TOP 5 des revues en logique.

2. J-M. Le Bars. The 0-1 law fails for frame satisfiability of propositional modal logic. In Proceedings of the 17th IEEE Symposium on Logic in Computer Science, 2002 , 225-234 Impact facteur 1,79 CORE : rang A*

   J'ai étendu mes résultats de contre-exemples de lois 0-1 à des logiques pour l'Intelligence artificielle. J'ai ainsi réfuté un résultat connu établi par Halpern et Kapron en 1994.

3. C. Bazin, J-M. Le Bars et J. Madelaine A Blind, Fast and Robust Method for Geographical Data Watermarking ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), Singapore, ACM SIGSAC, 2007, 265-272 Rang B

   Nous proposons dans cet article un algorithme de tatouage aveugle qui respecte la précision et la topologie des documents géographiques vectoriels . Cet algorithme découpe un document en sites définis à partir de la triangulation de Delaunay. Nous avons prouvé expérimentalement que cet algorithme résiste à des transformations naturelles telles que la rotation et le découpage.

4. J-M. Le Bars and A. Viola. Equivalence classes of Boolean functions for first-order correlation. IEEE Transactions on Information Theory, 56 (3), 1247 -1261, 2010. Impact factor 2,6 CORE Rang A*

   Cet article de journal reprend les premiers résultats que nous avons eus avec Viola sur les fonctions booléennes, celles-ci sont manipulées par classes d'équivalence, ce qui nous permet de compter et énumérer toutes les fonctions 1-résilientes jusqu'à 7 variables.

5. B Z. Yao, J.M. Le Bars, C. Charrier, C. Rosenberger, "Quality Assessment of Fingerprints with Minutiae Delaunay Triangulation", International Conference on Information Systems Security and Privacy (ICISSP), 2015 (taux de sélection : 20%).

   Je co-encadre (25 %) la thèse de Zhigang YAO avec C. Rosenberger et C. Charrier. Il travaille sur l'évaluation de la qualité d'empreintes digitales. Dans ce papier, nous proposons une méthode permettant de qualifier la qualité d'une empreinte digitale uniquement à partir de l'ensemble des minuties avec une représentation basée sur une triangulation de Delaunay. Cette méthode est la première méthode de l'état de l'art ne traitant que des minuties en entrée (sans avoir accès à l'image de l'empreinte digitale).

4.8 Liste des publications

Habilitation à diriger les recherches

[1] J-M. Le Bars Quelques études de l'aléatoire en informatique, Normandie Université, juin 2016.

Thèse

[2] J-M. Le Bars Probabilités asymptotiques et pouvoir d'expression des fragments de la logique du second ordre, Université de Caen Normandie, janvier 1998.

Revues internationales avec comité de lecture

[3] Yao, J-M Le Bars, C. Charrier and C. Rosenberger, A Literature Review of Fingerprint Quality Assessment and Its Evaluation, To IET Biometrics journal,

[4] J-M Le Bars et A. Viola. Enumerative encoding of correlation-immune. Theoretical Computer science, 487, 23-36, 2013

[5] J-M. Le Bars et A. Viola. Equivalence classes of Boolean functions for first-order correlation. IEEE Transactions on Information Theory, 56 (3), 1247 -1261, 2010.

[6] J-M. Le Bars. The 0-1 law fails for the monadic existential second-order logic on undirected graphs Information Processing Letters, 77/43-48, 2001.

[7] J-M. Le Bars. Counterexamples of the 0-1 law for fragments of existential second-order logic : an overview. Bulletin of Symbolic Logic, 9 :67–82, 2000.

Actes de colloques internationaux avec comité de lecture

[8] Z. Yao, J. Le bars, C. Charrier, C. Rosenberger, Pixel Pruning for Fingerprint Quality Assessment, NIST International Biometric Performance Testing Conference (IBPC), 2016.

[9] Z. Yao, J-M Le Bars, C. Charrier and C. Rosenberger, Fingerprint Quality Assessment With Multiple Segmentation, workshop on Biometric Security of the international conference on Cyberworlds, 7-8 october 2015..

[10] M. Barbier, J-M Le Bars, C. Rosenberger, Image Watermaking With Biometric Data For Copyright Protection, workshop MFESC of the International Conference on Availability, Reliability and Security (ARES) Toulouse, France, 24-28 august 2015

[11] B. Vibert, J-M Le Bars, C. Charrier, C. Rosenberger, Comparative study of minutiae selection algorithms for ISO fingerprint templates, SPIE electronic imaging, 2015

[12] B. Vibert, J-M Le Bars, C. Charrier, C. Rosenberger, EvaBio Platform for the Evaluation Biometric System - Application to the Optimization of the Enrollment Process for Fingerprints Devices, ICISSP 2015

[13] Z. Yao, J-M Le Bars, C. Charrier and C. Rosenberger, Quality Assessment of Fingerprints with Minutiae Delaunay Triangulation, International Conference on Information Systems Security and Privacy (ICISSP 2015)

[14] Z. Yao, J-M Le Bars, C. Charrier and C. Rosenberger, Fingerprint Quality Assessment Combining Blind Image Quality, Texture and Minutiae Features, INSTICC 2015.

[[15] N. Carrasco, J-M Le Bars and A. Viola. Enumerative encoding of correlation-immune Boolean functions. IEEE Information Theory Workshop, Paraty, Brésil, 2011, 643-647.

[16] C. Bazin, J-M. Le Bars et J. Madelaine A Novel Framework For Watermarking : The Data-Abstracted Approach International Workshop on Security, IWSEC, 2008, 201-217.

[17] C. Bazin, J-M. Le Bars et J. Madelaine A Blind, Fast and Robust Method for Geographical Data Watermarking ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), Singapore, ACM SIGSAC, 2007, 265-272.

[18] J-M. Le Bars and A. Viola. Equivalence classes of boolean functions for first-order correlation. 2007 IEEE International Symposium on Information Theory (ISIT 2007), 181-186.

[19] C. Banderier, J-M. Le Bars, V. Ravelomanana. Generating Functions For Kernels of Digraphs (Enumeration & Asymptotics for Nim Games) In Proceedings of the 16th Annual International Conference on Formal Power Series and Algebraic Combinatorics (VancouversBC, Canada, June 28 - July 2 2004), 91-105.
[20] J-M. Le Bars. The 0-1 law fails for frame satisfiability of propositional modal logic. In Proceedings of the 17th IEEE Symposium on Logic in Computer Science, 2002, 225-234.
[21] J-M Le Bars, Fragments of Existential Second-Order Logic without 0-1 Laws. LICS 1998, 525-536.

Conférence nationale avec comité de lecture

[22] B. Vibert, J.M. Le Bars, C. Charrier, C. Rosenberger, "Définition du type d'empreinte à partir d'un template ISO Compact Card II", Colloque COmpression et REprésentation des Signaux Audiovisuels (CORESA), 2016
[23] M. Barbier, J-M Le Bars, C. Rosenberger, Image Watermaking With Biometric Data For Copyright Protection, APVP 2015 (Atelier sur la Protection de la Vie Privée), juin 2015, Mosnes.

4.8.1 Prix et distinctions

Prix international Kleene Award, prix du meilleur article étudiant, à la conférence internationale Logic in Computer Science (LICS'98) pour l' article *Fragments of existential second-order logic without 0-1 laws* en 1998.

Prix national Le jury du Prix de Thèse SPECIF 1998, présidé par Gilles Kahn de l'Académie des Sciences, m'a attribué un des deux accessits pour ma thèse.

4.9 Projet de recherche

Mon projet de recherche porte sur l'extraction d'aléatoire sur des données réelles pour des applications de différents domaines comme la cryptographie, la biométrie ou le tatouage. La modélisation aléatoire de données est souvent extrêmement complexe et parfois irréalisable en pratique, mais heureusement elle n'est pas nécessaire pour la plupart des applications. En effet, on souhaite pouvoir mettre en évidence des parties aléatoires sans avoir à fournir une modélisation complète. Mon objectif est double :

- d'une part, de fournir un cadre général (framework) et de pouvoir formaliser ce nouveau type d'étude. Il s'agit, en particulier, d'identifier les aspects généraux et ceux qui dépendent des applications envisagées. La constitution de ce framework devra probablement nécessiter quelques années.
- d'autre part, diverses pistes pourront être explorées en proposant des recherches expérimentales, plus pratiques et ciblées, à des étudiants en thèse ou en master.