1 Sous-équipe ATI : Arithmétique et Théorie de l'Information

1.1 Composition

Membres permanents (2011-2016) :
5 professeurs : A. Bonnecaze (responsable ATI), D. Kohel, P. Liardet (émérite, décédé en Août 2014), S. Louboutin, S. Vladut ;
4 maîtres de conférences : Y. Aubry, S. Ballet, R. Rolland (émérite), C. Ritzenthaler (départ Sept 2013) ;
3 DR CNRS : G. Lachaud (émérite), F. Rodier (émérite), M. Laurent (départ 2014) ;
1 CR CNRS : M. Balazard
Membres non permanents (2011-2016) :
Post-doctorants : S. Ram (contrat post-doctoral du LabEx Archimède 1/03/2013-30/06/2014)
Doctorants : A. Venelli (thèse soutenue le 31/01/2011), S. Haloui (thèse soutenue le 14/06/2011), C. Arène (thèse soutenue le 27/09/2011), J. Pieltant (thèse soutenue le 12/12/2012), Hamish Ivey-Law (thèse soutenue le 14/12/2012), M. Tukumuli (thèse soutenue le 13/09/2013), V. Ducet (thèse soutenue le 23/09/2013), Marc Munsch (thèses soutenue le 14/10/2013), S. Dib (thèse soutenue le 11/12/2013), F. Caullery (thèse soutenue le 28/05/2014), F. Rovetta (thèse soutenue le 4/12/2015), Y. Shieh (thèse soutenue le 17/12/2015), T. Alasha, A. Iezzi, A. Giangreco Maidana, H. Dang.

Nombre de départs de permanents (2011-2016) : 5
Nombre d'arrivées de permanents (2011-2016) : 0
Nombre de permanents (juin 2016) : 7 (4 professeurs et 2 maîtres de conférences, 1 CR CNRS)

1.2 Positionnement scientifique

L'équipe Arithmétique et Théorie de l'Information est née de la rencontre entre des chercheurs travaillant à l'interface entre la théorie des nombres, la géométrie algébrique et leurs applications à la Théorie de l'Information, notamment aux codes correcteurs d'erreurs et à la cryptographie, ce qui identifie les trois thèmes principaux sur lesquels travaille l'équipe. Ces trois thèmes interagissent entre eux. D'un autre point de vue, il faut aussi mentionner le fait que la recherche de l'équipe est à la frontière de la théorie des nombres effective, algorithmique, et computationnelle. Plus précisément, l'effectivité concerne l'existence de solutions algorithmiques pour traiter les problèmes tels que leur contenu est effectivement calculable. L'algorithmique concerne l'étude de l'efficacité des solutions, c'est-à-dire les problèmes de complexité essentiellement. Finalement, on peut distinguer, dans la théorie algorithmique des nombres, une sous-culture de la théorie des nombres à savoir la théorie des nombres dite computationnelle, dont l'objectif est de mettre en oeuvre les algorithmes, d'étudier les comportements en pratique (problèmes d'implémentation etc...) et éventuellement d'en tirer des conclusions théoriques par des expériences avec ordinateur.

Il faut noter qu'au sein de l'université d'Aix-Marseille, l'équipe ATI est la seule équipe à être aussi spécialisée dans le domaine de la cryptographie et avoir des compétences dans le domaine plus général de la sécurité des systèmes d'information.

D'un point de vue plus détaillé, voici les différents thèmes de recherche abordés par l'équipe ATI.

Théorie des nombres

- Théorie algébrique et analytique des nombres : hypothèse de Riemann, répartition de fonctions arithmétiques, corps de nombres (fonctions L, fonctions zêta, nombre de classes, unités fondamentales), distributions du Frobenius (Lang-Trotter et Sato-Tate conjectures), sommes exponentielles, cyclotomie des sommes de Weil, équations diophantiennes ;
- Théorie algorithmique des nombres : algorithmes dans les corps finis, dans les corps de nombres, les corps de fonctions et variétés algébriques (Chudnovsky, méthode CM, Comptage de points : algorithmes de Schoof-Elkies-Atkin, méthode p-adic de Satoh et Mestre par relèvement canonique, méthode p-adique de Kedlaya) ;

Géométrie algébrique

- Etude des propriétés géométriques et arithmétiques de différents objets géométriques (courbes, variétés abéliennes, surfaces,...), pour des applications à la théorie des codes et la cryptographie ;

- Arithmétique dans les corps de fonctions : tours/suites de corps de fonctions définis sur des corps finis (tours de type Kummer, Artin-Schreier, modulaires, Shimura), espaces de Riemann-Roch, problème de la descente ;

- Nombre de points rationnels d'ensembles algébriques, de variétés abéliennes dont les variétés de Prym et les jacobiennes sur les corps finis ;

- Courbes de petits genres ;

- Courbes singulières, courbes optimales et maximales ;

- Obstruction de Serre ;

- Cohomologie l-adique ;

- Questions de régularité des équations aux dérivées partielles de type elliptique et de type hydrodynamique.

Théorie de l'information

- Complexité algébrique (complexité des opérations arithmétiques dans les corps finis) ;

- Fonctions booléennes en codage et en cryptographie, non-linéarité, fonctions APN et fonctions de faible uniformité différentielle, étude asymptotique de l'uniformité différentielle ;

- Poids des codes de Reed-Muller généralisés, et des codes définis sur des variétés quadratiques ou hermitiennes ;

- Constructions de codes correcteurs pour des problèmes de transmission d'information utilisant de la géométrie algébrique et de la théorie des nombres. En particulier, il s'agit de codes avec différentes conditions de localité et de sparsité ;

- Cryptographie appliquée (construction et étude de primitives et protocoles cryptographiques, side channel, générateurs pseudo-aléatoires, partage de secret, dictionnaires authentifiés) ;

- Construction d'algorithmes d'exponentiation dans les corps finis ;

- Implémentation effective d'algorithmes.

L'équipe ATI est impliquée dans le master Mathématiques Discrètes et Fondements de l'Informatique (MDFI), dont le responsable est David Kohel. Ce master fait intervenir des membres de l'I2M, du LIF et de l'INRIA.

Les échanges entre les différents thèmes de l'équipe sont réguliers et fructueux. Les relations avec l'extérieur sont fortes et nombreuses grâce aux collaborations individuelles dans les thématiques de l'équipe et en dehors.

1.3 Réalisations

1.3.1 Production scientifique

Au cours de la période, l'équipe a publié près de 100 ouvrages et articles. Les chercheurs de ATI publient notamment dans les journaux suivants : journal of algebra, journal of number theory, Moscow mathematical journal, journal of complexity, mathematics of computation.

Quelques problèmes qui sont au cœur de la recherche de l'équipe concernent les calculs des invariants d'ensembles algébriques ou de variétés (surtout des courbes ou des variétés abéliennes) sur un corps fini ou de corps des nombres. Les problèmes traités incluent les groupes de points rationnels des variétés abéliennes, en particulier des Jacobiennes, ou la détermination et la structure des groupes de classes et des groupes des unités des corps de nombres.

Pour les variétés sur les corps finis, la détermination des invariants se synthétise en la détermination de la fonction zêta (nombre de classes, de diviseurs effectifs, nombre de points rationnels sur les extensions de base à l'aide d'algorithmes de comptage). Ce problème joue un rôle essentiel dans l'utilisation des courbes et variétés abéliennes en cryptographie. Plusieurs membres de l'équipe tels que Yves Aubry (et sa doctorante Safia Halloui), Stéphane Ballet, David Kohel, Gilles Lachaud et Robert Rolland ont apporté des contributions essentielles dans ce secteur.

Pour les groupes de classes, les bornes effectives jouent un rôle important. On généralise ce problème à l'étude des propriétés des fonctions-L d'un corps de nombres. On peut citer le problème du nombre de classes égal à 1 comme problème type dans ce domaine. Le travail de Stéphane Louboutin est très important dans cette discipline.

Une autre direction importante de l'équipe (en particulier David Kohel et Christophe Ritzenthaler ainsi que leur doctorant Florent Rovetta) en collaboration avec d'autres membres du laboratoire (par exemple Boris Kolev et Marc Olive) est la théorie des invariants proprement dite à savoir déterminer des invariants d'une courbe qui permet de distinguer les classes d'isomorphismes, et le problème inverse, produire une courbe représentative à partir de ces invariants. Ce thème est non seulement complémentaire avec les thèmes précédents mais aussi a des applications en physique théorique.

Notons aussi sur ce dernier point concernant les applications en physique théorique les travaux remarquables de Serge Vladut en collaboration avec Nikolai Nadirashvili. Ces travaux portent sur les constructions des solutions non-classiques et singulières pour les équations aux dérivées partielles uniformément elliptiques complètement non-linéaires.

Une direction de recherche récente de David Kohel, Gilles Lachaud et Yih-Dar Shieh (dans sa thèse) concerne des questions de distribution de Frobenius liées aux généralisations des conjectures de Sato-Tate et Lang-Trotter, qui surviennent en étudiant les fonctions zêta ou fonctions-L sur un corps de nombres ou dans une famille.

Une autre direction importante de recherche concerne le travail de François Rodier sur l'étude des fonctions booléennes.

Notons aussi qu'un membre de l'équipe, Yves Aubry, s'intéresse aussi à des problèmes de théorie des graphes, théorie dont on a pu mesurer l'intérêt dans la description de l'arbre de ramification pour la construction de tours de corps de fonctions algébriques atteigant Drinfeld-Vladut grâce aux travaux récents de Hallouin-Perret.

D'un point de vue plus détaillé, voici les résultats obtenus par thèmes de recherche par les membres de l'équipe :

Théorie des nombres Les résultats d'ATI appartiennent aussi bien au domaine de la théorie des nombres que de la théorie algorithmique des nombres.

En ce qui concerne la théorie des nombres :

Yves Aubry s'est intéressé à l'étude des sommes exponentielles, des groupes de monodromie et des points entiers de certaines équations diophantiennes.

- *Les sommes exponentielles.*

En collaboration avec Daniel Katz (California State University, Northridge) et Philippe Langevin (Université du Sud Toulon-Var), Yves Aubry a donné, via une approche à galoisienne, plusieurs résultats concernant des sommes de Weil à trois valeurs, généralisant notamment à toute caractéristique non nulle des résultats de Calderbank-McGuire-Poonen-Rubinstein, de Calderbank-McGuire et de Charpin établis en caractéristique 2.

D'autre part, Yves Aubry s'est intéressé, en collaboration avec Philippe Langevin, à une conjecture de Helleseth liant le déterminant d'une certaine fonction puissance au produit de ses coefficients de Fourier. En utilisant la théorie des caractères, ils ont démontré certaines propriétés de divisibilité allant dans le sens de cette conjecture.

- *Les groupes de monodromie.*

Yves Aubry a déterminé, en collaboration avec Fabien Herbaut (Université de Nice Sophia Antipolis), des groupes de monodromie géométrique et arithmétique, et, in fine, obtenu, via le théorème de densité de Chebotarev, un résultat de densité sur les polynômes d'uniformité différentielle du second ordre maximale.

Via l'approche de Voloch et l'étude des groupes de monodromies, Yves Aubry souhaite obtenir des polynômes à uniformité différentielle maximale. Cela permettra de cerner plus précisément les fonctions utilisables dans les boîtes S des cryptosystèmes.

- *Les équations diophantiennes.*

Yves Aubry et Dimitrios Poulakis se sont s'intéressés à la hauteur des solutions entières des équations de Thue. Ils ont considérablement amélioré les bornes connues sur la hauteur et le nombre de ces solutions entières. Enfin, ils ont obtenu un algorithme pour déterminer les solutions entières de telles équations.

Yves Aubry souhaite continuer à travailler sur la détermination de la hauteur des points entiers. Il espère que son approche des équations de Thue lui permettra d'obtenir des estimations de cette hauteur.

Michel Balazard a obtenu une nouvelle preuve d'une équation fonctionnelle approchée due à J.R. Wilton, pour une somme trigonométrique impliquant la fonction diviseur.

Michel Laurent, en collaboration avec un membre de l'équipe GDAC de l'I2M Arnaldo Nogueira, a utilisé l'approximation diophantienne et la mesure d'irrationnalité pour déterminer différents paramètres topologiques (dimension de Hausdorff, nature du point initial x de l'orbite $SL(2,Z)x$ lorsque x a une pente irrationnelle).

S. Louboutin travaille à la fois en théorie analytique des nombres (fonctions L et fonctions zêta de Dedekind) et théorie algébrique des nombres (unités fondamentales des ordres engendrés par une unité).

Pour le premier aspect, il a par exemple obtenu en 2000 la borne suivante souvent citée sur les résidus au point 1 de la fonction zêta de Dedekind d'un corps de nombre K de degré n et de valeur absolue de discriminant d_K :

$$\mathrm{Res}_{s=1}(\zeta_K(s)) \leq \left(\frac{e\log d_K}{2(n-1)}\right)^{n-1} \qquad (1).$$

Cette meilleure borne connue a, par une approche complètement différente, été en 2012 améliorée sans être rendue explicite par Xiannan Li . S. Louboutin à en 2015 publié une version explicite de ce résultat. Il en ressort que cette borne de X. Li, bien qu'asymptotiquement meilleure, est malheureusement d'un point de vue pratique inutilisable (puisque meilleure que (1) seulement pour des degrés ou des "root discriminants" de K élevés). Il y a donc un travail actuel en cours pour améliorer significativement (1). Une direction est de prendre en compte le comportement des petits nombres premiers dans K. Couplé avec le résultat de S. Louboutin publié en 2015 sur les zones du type $[1-c_m/\log d_K, 1[$ sur lesquelles les fonctions $\zeta_K(s)$ ont au plus un nombre donné m de zéros, un tel résultat suffisamment bon et complètement explicite, ne serait-ce que pour les corps cubiques non galoisiens, pourrait enfin sans doute permettre de résoudre le problème du nombre de classes 1 pour les corps à multiplication complexe de degré 6.

Pour le second aspect, soit ε une unité algébrique qui n'est pas une racine de l'unité. Si le groupe des unités de l'ordre $\mathbf{Z}[\varepsilon]$ est de rang 1 (c'est à dire si ε est (i) quadratique réelle, (ii) cubique non totalement réelle ou (iii) quartique totalement imaginaire), est-il vrai que ε est une unité fondamentale de cet ordre ? Suite aux travaux récents de S. Louboutin et d'autres auteurs, ce problème est maintenant résolu. Pour les cas où le rang r du groupe des unités de l'ordre $\mathbf{Z}[\varepsilon]$ est supérieur ou égal à 2, la question naturelle est maintenant : existe-il toujours $r-1$ unités $\varepsilon_2,\cdots,\varepsilon_r \in \mathbf{Z}[\varepsilon]$ telles que les r unités $\{\varepsilon,\varepsilon_2,\cdots,\varepsilon_r\}$ forment un système d'unités fondamentales de l'ordre $\mathbf{Z}[\varepsilon]$? En 2010, S. Louboutin a commencé à aborder cette question pour le cas $r=2$ en y répondant complètement dans le cas où ε est cubique totalement réelle. Il travaille actuellement sur le cas difficile des unités quartiques de discriminant négatif, cas où ici encore $r=2$. Il a en 2015 publié un long état des lieux (avec preuves de tous les résultats connus à ce jour) de la recherche sur ces questions.

En ce qui concerne la théorie algorithmique et computationnelle des nombres :

Un noyau dur s'est progressivement formé depuis 2011 sous l'impulsion de Stéphane Ballet et Alexis Bonnecaze. Ce groupe comprend Kévin Atighehchi (ATER membre du LIF), Stéphane Ballet, Nicolas Baudru (chercheur membre du LIF), Alexis Bonnecaze, Robert Rolland auquel s'est ajouté plusieurs doctorants (Julia Pieltant, Mila Tukumuli, Hung Dang) et s'ajoutera une post-doctorante en début 2017 (Selda Çalkavur). Il s'intéresse à l'arithmétique rapide sur les corps finis et a pour objectif de mieux comprendre et d'ainsi améliorer (en terme de complexité) les algorithmes de multiplication de type Chudnovsky qui sont basés sur l'interpolation à partir de courbes algébriques définies sur un corps fini. Le problème de l'amélioration de la complexité totale est lié au choix des espaces de Riemann-Roch $\mathscr{L}(D)$ et $\mathscr{L}(2D)$ dans l'algorithme de D.V. et G.V. Chudnovsky (c'est à dire le choix du diviseur D et le choix de la base de représentation des espaces associés). En 2015, à partir d'un travail sur la représentation de ces espaces, le groupe a amélioré des résultats obtenus en 2009 par Couveignes et Lercier.

Par ailleurs, Stéphane Ballet et Julia Pieltant ont obtenu des bornes uniformes de la complexité bilinéaire de la multiplication dans toute extension de $\mathbb{F}_2$ grâce à des techniques de descente du corps de définition de tours non-ordinaires de corps de fonctions de type Garcia-Stichtenoth atteignant la borne de

Drinfeld-Vladut ainsi que de l'existence de diviseurs de dimension nulle de degré proche de $g-1$. Récemment, en utilisant des tours de corps de fonctions ayant un invariant de Hasse-Witt maximal, ils ont pu améliorer les bornes de la complexité bilinéaire de la multiplication dans toute extension de $\mathbb{F}_2$ grâce à l'existence de diviseurs non-spéciaux de degré g-1.

Dans le domaine du problème de comptage des points rationnels d'une courbe, David Kohel a obtenu des résultats sur le comptage des points rationnels de courbes elliptiques ainsi que des généralisations sur les Jacobiennes des courbes de genre 2. D'autre part, le travail de David Kohel sur les lois de groupe des courbes elliptiques et variétés abéliennes comporte des avancées mathématiques théoriques qui ont donné lieu à des algorithmes efficaces dans une perspective d'application à la cryptographie.

Dans le domaine de la théorie des nombres computationnelle, David Kohel a apporté des contributions au système de calcul formel Magma et Sage.

Géométrie algébrique Les thèmes de géométrie algébrique ainsi que ceux traités dans la section Théorie de l'Information sont intimement liés dans notre équipe. En particulier, un certain nombre de problèmes de géométrie algébrique pure sont directement issus de problématiques liées à l'arithmétique efficace dans les corps finis.

L'équipe a apporté des contributions dans les domaines des courbes algébriques ainsi que des variétés abéliennes. Nous présentons les principaux faits pour chacun des domaines.

a) Courbes algébriques, familles de courbes algébriques et corps de fonctions associés

Yves Aubry a étudié en collaboration avec Annamaria Iezzi le nombre maximal de points rationnels sur un corps fini d'une courbe algébrique projective de genres géométrique et arithmétique fixés. En suivant des idées de Rosenlicht et de Serre, ils ont travaillé sur le spectre des anneaux locaux des courbes lisses afin de construire des courbes singulières à singularités prescrites, et notamment possédant beaucoup de points rationnels vis à vis de leurs genres (ils ont notamment généralisé des résultats de Fukasawa-Homma-Kim établis en 2012).

D'autre part, en utilisant une approche euclidienne développée par Hallouin-Perret en 2014 dérivée du théorème de l'indice de Hodge, ils ont établi une nouvelle borne supérieure pour le nombre de points fermés de degré 2 d'une courbe lisse. Ceci leur a permis d'établir des conditions suffisantes pour la non-existence de courbes optimales. Enfin, ils ont étudié le spectre des genres des courbes singulières maximales généralisant les résultats de Ihara, Rück, Stichtenoth, Fuhrmann, Garcia, Torres, Abdòn et Korchmáros.

Gilles Lachaud a étudié la distribution de la fonction trace sur le groupe symplectique unitaire. Cette distribution intervient dans les propriétés d'équidistribution pour les valeurs propres du Frobenius de familles de variétés abéliennes sur les corps finis, et dans la distribution limite du nombre de points normalisé des familles de courbes. Il a donné, à l'aide de fonctions spéciales, quatre expressions de la distribution de la trace si $g = 2$, et aussi, avec David Kohel, une expression de cette distribution en termes de fonctions symétriques élémentaires.

Gilles Lachaud a par ailleurs étudié la distribution de la fonction trace de la représentation de dimension 7 du groupe de Lie semi-simple compact de type G_2. Cette distribution intervient dans les propriétés d'équidistribution d'une famille de sommes exponentielles construite à partir de certains polynômes de degré 7. On l'obtient en calculant tout d'abord le simplexe fondamental des classes de conjugaison de G_2. En appliquant la formule d'intégration de Weyl, on obtient une formule exacte pour la densité de la distribution de la trace. Ceci répond à une question posée par J.-P. Serre et N. M. Katz.

Stéphane Ballet et Robert Rolland ont collaboré avec Seher Tutdere (Université de Gebze, Turquie) afin de construire des tours de corps de fonctions définis sur des corps finis (tours de type Kummer, Artin-Schreier, modulaires, Shimura) ayant un ou plusieurs invariants de Drinfeld-Vladut positifs : bornes sur le genre, bornes sur le nombre de places de différents degrés, descente du corps de définition, bornes sur le nombre de classes.

b) Variétés abéliennes

Yves Aubry, Safia Haloui et Gilles Lachaud ont établi de nouvelles majorations et minorations pour le nombre de points rationnels des variétés abéliennes et des Jacobiennes sur un corps fini. Ils ont de plus déterminé les nombres maximum et minimum de points rationnels des surfaces Jacobiennes sur un corps fini donné.

D'autre part, Yves Aubry et Safia Haloui ont considéré une autre classe de variétés abéliennes : les variétés de Prym associées aux revêtements double non ramifiés. Ils ont établis de nouvelles bornes concernant leur nombre de points rationnels améliorant les résultats de Perret.

Enfin, utilisant la construction de Legendre développée par Mumford décrivant les revêtements doubles non ramifiés des courbes hyperelliptiques, ils ont prouvé que le produit de deux courbes elliptiques muni de sa polarisation produit est isomorphe à une variété de Prym sauf dans quelques cas particuliers. Il en ont déduit les nombres de points rationnels maximum et minimum des surfaces de Prym.

Stéphane Ballet et Robert Rolland ont obtenu des bornes inférieures sur le nombre de points des Jacobiennes de tous les étages de tours de corps de fonctions algébriques de type Garcia-Stichtenoth ayant un ou plusieurs invariants de Drinfeld-Vladut positifs. D'un point de vue asymptotique, ils ont montré que ces bornes sont optimales dans le sens qu'elles atteignent la borne inférieure du Théorème de Brauer-Siegel Généralisé. Une partie de ces travaux ont été faits en collaboration avec Seher Tutdere.

Gilles Lachaud et Robert Rolland, ont obtenu des majorations du nombre de points d'un ensemble algébrique affine ou projectif, défini sur une extension d'un corps fini par un système d'équations polynomiales, y compris dans le cas où l'ensemble algébrique n'est pas défini sur le corps fini lui-même. Une attention particulière a été portée aux ensembles algébriques irréductibles mais non absolument irréductibles, pour lesquels ils obtiennent de meilleures bornes. Ils ont étudié le cas des intersections complètes, pour lesquelles ils ont construit une décomposition moins fine que la décomposition en composantes irréductibles, mais plus directement liée aux polynômes qui définissent l'ensemble algébrique en question. Enfin, ils ont construit des familles d'ensembles algébriques atteignant le nombre maximum de points rationnels dans le cas affine, et comportant de nombreux points dans le cas projectif.

Théorie de l'information Dans le domaine de la théorie de l'information, ATI s'intéresse principalement aux codes correcteurs d'erreurs, à la cryptographie, l'algorithmique et la théorie des graphes.

a) Codes correcteurs d'erreurs

Stéphane Ballet et Robert Rolland ont apporté une contribution à l'étude des mots de poids faibles des codes de Reed-Muller affines et projectifs généralisés.

François Rodier a utilisé des techniques probabilistes de convergence uniforme et de grandes déviations ainsi que des résultats de Katz et Sarnak et Deligne sur l'équidistribution des valeurs du nombre de points de certaines courbes pour définir une stratégie pour prouver la conjecture sur les rayons de recouvrement des codes de Reed-Muller en dimensions impaires.

Serge Vladut a construit des codes avec des propriétés de correction locale très exigeantes (les codes LRC) à partir de courbes possédant un grand nombre de points rationnels sur un corps fini. Ces constructions généralisent la construction de Barg-Tamo des codes optimaux LRC (2014), qui utilise les polynômes et donc essentiellement la droite projective comme une courbe de base. Elles permettent de construire de très nombreuses classes des codes LRC. L'étude asymptotique (lorsque la longueur tend vers l'infini) de ces constructions permet d'obtenir des codes dépassant différentes bornes de type Gilbert-Varshamov pour les codes LRC.

Serge Vladut a par ailleurs construit des analogues en théorie de codage de matrices de type "compressed sensing". La théorie de "compressed sensing" concerne essentiellement les codes (via leur matrices génératrices) sur les réels. La transposition directe de ces codes au cas des codes correcteurs d'erreurs sur un corps fini n'est pas possible. Toutefois, on peut formuler des conditions sur les CCE qui transposent "compressed sensing" dans ce contexte grâce à une condition sur les syndrômes. Ceci permet de construire des codes intéressants pour ce problème avec des paramètres très satisfaisants.

b) Cryptographie

Avec une doctorante, François Rodier a développé une étude fine de la distribution de la non-linéarité des fonctions booléennes, notamment la r-non-linéarité, qui est la distance de f aux fonctions de degré r. C'est un problème qui se pose pour améliorer la resistance aux différentes attaques d'un systèmes de cryptographie à flot. Il a également étudié la distribution de la non-linéarité des fonctions booléennes vectorielles, qui interviennent dans les boîtes de substitution en cryptographie par blocs.

L'étude de la non-linéarité des fonctions booléennes a permis en outre de préciser les bornes au delà desquelles on ne peut plus corriger d'erreurs dans le décodage des codes de Reed et Muller.

Cette étude a amené François Rodier à considérer les fonctions booléennes à valeurs dans un espace vectoriel sur $\mathbb{F}_2$. Ces fonctions servent en particulier à construire des “boites-S" pour implanter des cryptosystèmes de chiffrement symétriques, du type DES ou AES. Il a montré un critère sur le degré permettant de dire que certaines fonctions n'étaient pas presque parfaitement non-linéaires (APN). Cette propriété caractérise la résistance à certaines attaques dites différentielles.

François Rodier et Yves Aubry ont formulé avec McGuire (University College Dublin) la conjecture suivante : *Un polynôme ne peut être APN pour une infinité de corps $\mathbb{F}_q$ que si il est équivalent à un monôme x^t lorsque t est un exposant exceptionnel.* Cette conjecture a déjà été vérifiée pour un certain nombre de cas.

Après une étude supplémentaire, une des fonctions booléennes ainsi mises en évidence pourrait être candidate pour être un composant d'un successeur de l'AES.

Plusieurs membres d'ATI se sont intéressés à l'étude et la construction de générateurs pseudo-aléatoires. Robert Rolland et Stéphane Ballet ont travaillé sur le théorème de Yao. Alexis Bonnecaze et Pierre Liardet on construit un générateur k parmi n uniforme de type Monte Carlo utilisant des objets combinatoires et des marches aléatoires. Ces derniers résultats ont illustré un cours intitulé "Aléas et cryptographie avec un point de vue dynamique" donné à l'école thématique Théorie des nombres et Dynamique durant l'été 2013 à l'Institut Fourier.

Gilles Lachaud a lui aussi obtenu des résultats dans le domaine des générateurs pseudo-aléatoires et plus particulièrement les registres à décalage vectoriels (ou σ-LFSR) qui ont été introduits par Zeng. On les construit à l'aide de matrices compagnons en blocs à coefficients dans un corps fini. Ils permettent une encryption beaucoup plus rapide que les registres à décalage usuels. Gilles Lachaud a décrit la structure algébrique des matrices compagnons en blocs ayant un polynôme caractéristique donné.

Dès 2009, Alexis Bonnecaze et son doctorant Alexandre Venelli (actuellement ingénieur à Thalès Communications & Security) se sont intéressés aux attaques par canaux cachés. Avec Pierre Liardet, ils ont proposé une modification de l'AES lui permettant d'être robuste face à une attaque par canaux cachés différentielle de premier ordre.

En 2014, Alexis Bonnecaze et Kévin Atighehchi, alors doctorant à l'I2M, ont proposé un modèle de dictionnaires authentifiés prenant en compte la fréquence d'accès aux données et qui permet de réduire la taille de la preuve cryptographique d'authentification.

En matière de cryptographie asymétrique, Robert Rolland et Dimitrios Poulakis (Aristotle University of Thessaloniki) ont proposé plusieurs protocoles liés aux échanges de clés et à la signature numérique.

c) Algorithmique

Grâce à une nouvelle construction de l'algorithme de multiplication de type Chudnovsky, Kévin Atighehchi, Stéphane Ballet, Alexis Bonnecaze et Robert Rolland ont décrit un algorithme efficace pour l'exponentiation et la multiplication dans des corps finis qui est fortement parallélisable. Ils ont analysé cet algorithme suivant trois modèles de complexité et l'ont comparé avec celui de Couveignes et Lercier de 2009. Ils ont montré en particulier qu'il est plus facile à paralléliser et qu'il a une meilleure complexité bilinéaire. Cependant, cet algorithme ne permet pas le traitement direct des extensions de $\mathbb{F}_q$ pour $q < 9$ et un objectif est de le généraliser aux extensions de petits corps. Un autre objectif est de le généraliser dans une autre direction, en utilisant des transformations k-linéaires de façon à internaliser le processus d'exponentiation, limitant ainsi le coût des entrées-sorties dans l'algorithme de Chudnovsky. Par ailleurs, la thématique souhaite travailler sur la détermination exacte de la complexité bilinéaire dans des extensions de $\mathbb{F}_{q^n}$. Pour cela, il est prévu d'étudier certains codes presque MDS de type $[2n, n, n+1]_{\mathbb{F}_q}$ car cette détermination exacte est liée à l'existence de ces codes. Ce travail sera effectué avec un doctorant et une post-doctorante.

c) Théorie des graphes

En collaboration avec Jean-Christophe Godin et Olivier Togni (Le2i, université de Bourgogne), Yves Aubry a tout d'abord décrit l'ensemble solution des poids possibles d'une coloration pour un graphe et une liste donnés.

Ils se sont intéressés par la suite aux sous-graphes induits sans triangle du réseau triangulaire. En lien avec les conjectures de Erdös-Rubin-Taylor et McDiarmid-Reed, ils ont démontré que, pour tout $m \geq 1$,

tout sous-graphe induit sans triangle du réseau triangulaire est $(5m, 2m)$-choisissable. Ils ont également étendu la notion de coeur d'un graphe et montré que la choisissabilité d'un graphe se réduit à celle de son coeur étendu.

Travaux transdisciplinaires En collaboration avec des géographes (des universités Blaise Pascal de Clermont-Ferrand et de Nouvelle Calédonie), Stéphane Ballet a aidé au traitement de l'information sur le plan statistique de données portant sur les espèces natives végétales dans les atolls de la Polynésie Française, espèces dont la densité est influencée par des critères abiotiques.

Serge Vladut a travaillé en collaboration avec Nikolai Nadirashvili. Ces travaux portent sur les constructions des solutions non-classiques et singulières pour les équations aux dérivées partielles uniformément elliptiques complètement non-linéaires. Dans ce domaine l'application des algèbres non-commutatives et non-associatives permet de contruire systématiquement un grand nombre de solutions homogènes non-classiques et singulières pour cette classe des EDP avec toutes les régularités possibles compatibles avec les resultats classiques de Caffarelli-Trudinger sur la régularité des solutions faibles ("viscosity solutions") et en toutes dimensions admises pour de telles solutions, sauf la dimension 4 restant inconnue. Remarquons que l'existence même de telles solutions est restée inconnue pendant plusieurs decénnies jusqu'en 2007 (travaux des mêmes auteurs).

1.3.2 Rayonnement et attractivité académiques

Durant la période 2011-2016, plusieurs membres d'ATI ont été membres de groupes de recherche (GDR-IM, C2, STN, GAGC).

Communications sur invitation en colloque ou séminaire international :

Les membres d'ATI on donné plus de 30 communications sur invitation en colloques.

Yves Aubry :

• Algebraic geometry for coding theory and cryptography, Institut for Pure and Applied Mathematics (IPAM), University of California Los Angeles (UCLA), USA, *Number of points of algebraic sets*, February 22-26th 2016.

• Algebra Days Conference (Antalya, Turquie), *On abelian varieties over finite fields*, 09-13 mai 2014.

• Algebraic Geometry and Coding Theory - India Conference (India, Bombay), *On three-valued Weil sums*, 02-06 december 2013.

Stéphane Ballet :

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

Alexis Bonnecaze :

• Invitation par le département de mathématiques de l'université de Jeddah (KAU, Arabie Saoudite). *Arithmetic in Finite Fields based on Chudnovsky Multiplication algorithms*, Octobre 2014.

Gilles Lachaud :

• AGCT-13 [Algebraic Geometry and Coding Theory] (CIRM, Luminy). 14-18 mars 2011.
Word oriented LFSR and construction of block Frobenius matrices in a given conjugacy class.

• Geocrypt 2011 (La Marana, Corse). 19-24 juin 2011.
Word oriented LFSR and construction of block Frobenius matrices in a given conjugacy class.

• CAAG 2012 (Pondicherry, Inde). 5-9 mars 2012.
Jacobians among abelian threefolds.

• AGCT-14 (CIRM, Luminy). 3-7 juin 2013.
On the number of points on abelian and Jacobian varieties over finite fields.

• CAI-5 [Conference on Algebraic Informatics] (Porquerolles). 3-6 septembre 2013.
Word oriented LFSR and construction of block Frobenius matrices in a given conjugacy class.

• AGCT-India (IIT Bombay, Inde) 2-6 décembre 2013.
Asymptotic distribution of the number of points of curves over a finite field.

• Frobenius distributions on curves (CIRM, Luminy). 24-28 février 2014.
Formulas for the limiting distribution of traces of Frobenius.

• Algebraic Geometry and Number Theory (Lab. Poncelet, Moscou). 23-27 juin 2014.
On the limiting distributions of traces of Frobenius.

• AGCT-15 (CIRM, Luminy) 18-22 mai 2015.
On the number of points of algebraic sets over finite fields.

• Arithmetic Geometry : Explicit Methods. (Lab. Poncelet, Moscou). 7-11 décembre 2015.
Distribution of the trace in UG2. Application to exponential sums.

• AGC [Algebraic Geometry and Coding] (IPAM, Los Angeles). 22-26 février 2016.
On the number of points of algebraic sets over finite fields.

Michel Laurent :

• Conférence "Diophantische Approximationen", *Inhomogeneous approximation and lattice orbits*, Oberwolfach (Avril 2012).

• Conférence "ERC research period on Diophantine Geometry", *Exponents of inhomogeneous approximation by lattice orbits*, Centro de Giorgi (Pise, Octobre 2012).

• Conférence "Heights and Diophantine Geometry, group theory and additive combinatorics", *Multidimensional approximation by primitive points*, Institut Schroedinger et Université de Vienne (Novembre 2013)

Stéphane Louboutin :

• 22st Czech and Slovak International Conference on Number Theory (2015, Slovakia). Exposé long de 45mn : Explicit upper bounds for residues of Dedekind zeta functions. 31/08- 04/09 2015.

David Kohel :

• Coding and Cryptology — Third International Workshop (IWCC 2011, Quingdao), *Arithmetic of split Kummer surfaces : Montgomery endomorphism of Edwards products*, 30 mai – 3 juin 2011.

• Theoretical and Practical Aspects of the Discrete Logarithm Problem (DLP 2014), *On the quaternion l-isogeny path problem*, Centro Stefano Franscini, Monte Verita, Ascona, Suisse, 4-9 mai 2014.

• Sage Days 61 : Quaterion Orders and Brandt Modules, University of Copenhagen, *Brandt modules*, 25–29 août 2014.

Christophe Ritzenthaler :

• Workshop on computational problems in number theory, Tianjin, Chine. Août 2015
• FoCM, Montevideo, Uruguay. Dec. 2014
• Antalya Algebra Days, Antalya, Turquie. Mai. 2014
• Algebraic curves over finite fields, Linz, Autriche. Nov. 2013
• Mathematical aspects of curves over finite fields, Oldenburg, Allemagne. Jui. 2013

François Rodier :

• Microsoft Research, Summer Number Theory Day, *Asymptotic nonlinearity of Boolean functions*, juillet 2012.

• Microsoft Research, Summer Number Theory Day, *Highly resistant Boolean functions for cryptography*, juillet 2012.

Communications sur invitation en colloque national :

Stéphane Ballet :

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

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

Gilles Lachaud :

• Crypto'Puces 2013 (Porquerolles). 27-31 mai 2013.
Word oriented LFSR and construction of block Frobenius matrices in a given conjugacy class.

Stéphane Louboutin :

• 9 Septembre 2014. Exposé d'une heure à la Conférence en l'honneur des 60 ans de J. F. Jaulent. Bordeaux : *Unités fondamentales des ordres engendrés par une unité*.

David Kohel :

• Journée Annuelle de la SMF, Arithmétique et dynamique : chaires Jean-Morlet 2014 *Théorie des nombres et cryptographie*, 20 juin 2014.

Communications sur invitation en école internationale :

Gilles Lachaud :

IIT Bombay (Mumbai, India). 27 février 2012.
Word oriented LFSR and construction of block Frobenius matrices in a given conjugacy class.

Exposés lors de séminaires :

Les membres d'ATI on donné plus de 14 exposés lors de séminaires.

Yves Aubry :

• Séminaire Algébrique de l'Université de Toulon : *Théorème de l'indice de Hodge et courbes maximales*, 03 novembre 2015.

• Séminaire Algébrique de l'Université de Toulon : *Nombre de points des variétés de Prym II*, 16 décembre 2014.

• Séminaire de Théorie des Nombres de l'Université de Caen : *Variétés de Prym sur les corps finis*, 12 décembre 2014.

• Séminaire Algébrique de l'Université de Toulon : *Nombre de points des variétés de Prym I*, 09 décembre 2014.

• Séminaire Algébrique de l'Université de Toulon : *Solutions entières d'une classe d'équations de Thue*, 30 septembre 2014.

• Séminaire Algébrique de l'Université de Toulon : *Equations diophantiennes et méthodes transcendantes*, 11 février 2014.

• Séminaire Algébrique de l'Université de Toulon : *Nombre de points rationnels des variétés de Prym*, 19 mars 2013.

Stéphane Ballet :

• Séminaire INFRES, Département Informatique et Réseaux (INFRES), Laboratoire Communications et Traitement de l'Information (LCTI), Groupe Mathématiques de l'Information, des Communications et du Calcul (MIC2), Telecom ParisTech, Paris : *Tours ordinaires de corps de fonctions et rang de tenseur de la multiplication dans les extensions de* $\mathbb{F}_2$ *et* $\mathbb{F}_3$, 7 juillet 2015.

Alexis Bonnecaze :

• Séminaire d'Informatique et Algèbre Appliquée, Institut de Mathématique de Toulon. *Exponentiation dans les corps finis basé sur l'algorithme de multiplication de Chudnovsky*, 6 mai 2014.

Gilles Lachaud :

• Séminaire ATI (IML, Luminy).
Distribution asymptotique du nombre de points des courbes sur un corps fini. 28 mars 2013.

• Séminaire ATI (I2M, Luminy).
Distribution of the trace in UG2. Application to exponential sums. 28 janvier 2016.

Stéphane Louboutin :

• Séminaire de Théorie des Nombres de Besançon : *Unités fondamentales des ordres engendrés par une unité algébrique*. 28 Juin 2012.

• Séminaire de Théorie des Nombres de l'Université de Caen : *Unités fondamentales des ordres engendrés par des unités*. 9 Janvier 2015.

• Séminaire de Théorie des Nombres de l'Université de Limoges : *Unité fondamentale des ordres engendrés par une unité*. 8 Juin 2015.

Encadrement doctoral

Les membre d'ATI ont fait soutenir 13 thèses.

Yves Aubry :

• Thèse de Safia Haloui en géométrie algébrique sur les variétés abéliennes et plus particulièrement les jacobiennes (thèse débutée le 1er septembre 2007 et soutenue le 14 juin 2011).

• Thèse d'Annamaria Iezzi à l'université d'Aix-Marseille, en géométrie algébrique, intitulée : Courbes algébriques projectives maximales sur les corps finis (bourse du Labex Archimède ; thèse débutée le 1er octobre 2012 ; soutenance prévue en 2016).

Stéphane Ballet :

• Co-direction (avec A. Bonnecaze) de la Thèse de Doctorat de Thanh-Hung DANG (en cours depuis mars 2016) : *Arithmétique efficace basée sur des courbes algébriques sur des corps finis*.

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

• Direction de la Thèse de Doctorat de Julia Pieltant (actuellement en Post-doctorat à Telecom ParisTech, Département INFRES Informatique et Réseaux) de septembre 2009 au 12 décembre 2012 (date de soutenance) : *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis*.

Alexis Bonnecaze :

• Thèse CIFRE (avec l'entreprise ATMEL) de A. Venelli, Contribution à la sécurité physique des cryptosystèmes embarqués. Rapporteurs : M. Joye et D. Naccache. Début de Thèse Fev 2008, soutenance 31 Janv 2011.

Gilles Lachaud :

• Co-encadrement (avec David Kohel) de la thèse de Yih-Dar Shieh, *Arithmetic aspects of point counting and Frobenius distributions* (I2M).

Stéphane Louboutin :

• Marc Munsch, *Moments des fonctions thêta*. Thèse soutenue le 14/10/2013. Rapporteurs : D. Essouabri et M. Jutila.

David Kohel :

• Co-encadrement avec C. Ritzenthaler de la thèse de Christophe Arene (bourse AXA). *Géométrie et arithmétique explicites des variétés abéliennes et applications à la cryptographie*. La thèse a été soutenue le 27 septembre 2011.

• Hamish Ivey-Law (codirecteur C. Fieker), *Algorithmic aspects of hyperelliptic curves and their jacobians*, U. Aix-Marseille et U. Sydney, 2012.

• Virgile Ducet, U. Aix-Marseille, 2013.

• Florent Rovetta (codirecteur C. Ritzenthaler), *Etude arithmétique et algorithmique de courbes de petit genre*, La thèse a été soutenue le 4 décembre 2015.

• Yih-Dar Shieh (codirecteur G. Lachaud), U. Aix-Marseille, 2015.

Christophe Ritzenthaler :

• Co-encadrement de la thèse de Yvan Ziegler avec Bernard Le Stum. *Points rationnels sur les courbes singulières*, Sep. 2013 -.

François Rodier :

• Stéphanie Dib. *Sur la distribution de la non-linéarité des fonctions booléennes*, soutenue en décembre 2013.

• Florian Caullery. *Sur les fonctions booléennes vectorielles presque parfaitement non-linéaire*, soutenue en mai 2014.

Serge Vladut :
• Giangreco Alejandro. *Groupes des points rationnels de surfaces abeliennes*, 2015-.

Jurys de thèse
Les membres d'ATI ont participé à plus de 40 jurys de thèses différents.

Yves Aubry :
• Florian Caullery de l'Université d'Aix-Marseille. *Fonctions planaires et presque parfaitement non linéaires* dirigée par François Rodier, le 28/05/14.
• Mila Tukumuli de l'Université d'Aix-Marseille. *Etude de la construction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis* dirigée par Alexis Bonnecaze, le 13/09/13.
• Mohamed Ould Douh Benioughde l'Université de Caen. *Corps de fonctions cyclotomiques* dirigée par Bruno Anglès, le 05/10/12.
• Elodie Leducq de l'Université Paris VII. *Autour des codes de Reed-Muller généralisés* dirigée par Jean-François Mestre, le 02/12/11.
• Mohamed Sall de l'Université Cheikh Anta Diop de Dakar. *Nouvelles constructions par sommes directes de codes cycliques projectifs à deux poids. Et dénombrement de codes cycliques irréductibles* dirigée par Cheikh Thiécoumba Gueye et Jacques Wolfmann, le 28/12/11.

Stéphane Ballet :
• Stéphanie Dib. *Distribution de la non-linéarité des fonctions booléennes*. 11 décembre 2013 à l'Université d'Aix-Marseille.
• Mila Tukumuli. *Etude de la contruction effective des algorithmes de type Chudnovsky pour la multiplication dans les corps finis*. 13 septembre 2013 à l'Université d'Aix-Marseille.
• Julia Pieltant. *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis*. 12 décembre 2012 à l'Université d'Aix-Marseille.
• Seher Tutdere dirigée par le Professeur Henning Stichtenoth, *On the asymptotic theory of function fields over finite fields*. 30 mai 2012 à Sabanci University à Istambul.

Alexis Bonnecaze :
• M. Rialha. *Routage et anonymité dans les réseaux ad hoc*, Université de Limoges, 2013. Rapporteur.
• B. Ait-Salem. *Sécurisation des réseaux Ad hoc : Systèmes de Confiance et de Détection de Répliques* Université de Limoges, 2011. Rapporteur.
• Irfana Memon. *Energy efficient secure and privacy preserving data aggregation in Wireless Sensor Networks*, 2013, Université d'Aix-Marseille.
• Laurent Vallet. *Contribution au renforcement de la protection de la vie privée ; Application à l'édition collaborative et anonyme des documents*, 2012, Université d'Aix-Marseille.

Gilles Lachaud :
• Safia Haloui. *Sur le nombre de points rationnels des variétés abéliennes sur les corps finis*. 14 juin 2011, IML.
• Christophe Arène. *Géométrie et arithmétique explicites des variétés abéliennes et applications à la cryptographie*, IML, 27 septembre 2011.
• Samrith Ram. *Singer Cycles, Coprime Polynomials, Hankel Matrices over Finite Fields and Arithmetic Progressions in Unique Factorization Domains*, Indian Institute of Technology, Mumbai, septembre 2011 (rapporteur).
• Julia Pieltant. *Tours de corps de fonctions algébriques et rang de tenseur de la multiplication dans les corps finis*, IML, Marseille, 2012.
• Virgile Ducet. *Construction of algebraic curves with many rational points over finite fields*. IML, Marseille, 23 septembre 2013.
• Stéphanie Dib. *Distribution de la non-linéarité des fonctions booléennes*. IML, Marseille, 11 décembre 2013.

• Romain Basson. *Arithmétique des espaces de modules de courbes hyperelliptiques de genre 3 en caractéristique positive*. Université de Rennes I, 25 juin 2015.

• Yih-Dar Shieh. *Arithmetic aspects of point counting and Frobenius distributions*, I2M, Marseille, 17 décembre 2015.

• Mrinmoy Datta. *Rational points on linear sections of algebraic varieties over finite fields and higher weights of linear codes*. Indian Institute of Technology, Mumbai, 2015 (rapporteur)

Stéphane Louboutin :

• Paloma Bengoechea, *Corps quadratiques et formes modulaires.* Soutenue le 3/07/2013 à Paris 6. Jury : P. Bayer, F. Brunault, W. Kohnen, S. Louboutin, L. Merel, N.-P. Skoruppa, D. Zagier.

• Marc Munsch, *Moments des fonctions thêta*. Soutenue le 14/10/2013 à Luminy. Jury : D. Essouabri, G. Lachaud, S. Louboutin, O. Ramaré, J. Rivat et E. Royer.

• Charlotte Euvrard, *Aspects explicites des fonctions L et applications*, sous la direction de Christian Maire. Rapporteur et membre du Jury. Date de soutenance programmée le 04/04/2016 à Besançon.

David Kohel :

• Enea Milio, *Calcul de polynômes modulaires en dimension 2*, U. Bordeaux, 2015.

• Kevin Atighehchi, *Contribution à l'efficacité des mécanismes cryptographiques*, U. Aix-Marseille, 2014.

• Christophe Tran, *Formules d'addition sur les jacobiennes de courbes hyperelliptiques : application à la cryptographie*, U. Rennes I, 2014. Rapporteur.

• Peng Tian, U. Roma, Tor Vergata, 2013. Rapporteur.

• Emmanuel Hallouin, HDR, U. Toulouse 2, 2013. Rapporteur.

• Kisoon Yoon, *Courbes elliptiques adoptées à la cryptographie à couplage*, U. Caen, 2013. Rapporteur.

• Jean-Gabriel Kammerer, *Analyse de nouvelles primitives cryptographiques pour les schémas Diffie-Hellman*, U. Rennes I, 2013. Rapporteur.

• Aurelien Bajolet, *Aspects numériques de l'analyse diophantienne*, U. Bordeaux, 2012. Rapporteur.

• Gaetan Bisson, U. Eindhoven, 2011. Rapporteur.

Christophe Ritzenthaler :

• Président du jury de la thèse d'Emmanuel Fouotsa sous la direction de S. Duquesne, Université Rennes 1. 2013.

• Virgile Ducet sous la direction de D. Kohel, Université d'Aix-Marseille. 2013.

• Muhammad Afzal Soomro sous la direction de J. Top, Université de Grönigen, Pays-Bas. 2013. Rapporteur.

• Hamish Ivey-Law sous la direction de D. Kohel, Université d'Aix-Marseille. 2012.

• Abdoul Aziz Ciss sous la direction de D. Sow, Université de Dakar, Sénégal. 2012. Rapporteur.

• Safia Haloui sous la direction de Y. Aubry, Marseille. 2011.

• Vijaykumar Singh sous la direction de G. McGuire, Dublin, Irlande. 2011. Rapporteur.

François Rodier :

• Julia Pieltant, Marseille, 2012.

• Hamish Ivey-Law, *Algorithmic aspects of hyperelliptic curves and their jacobians*, Marseille, 2012.

• Deng Tang, *Fonctions booléennes pour les schémas cryptographiques par flots et par blocs*, Paris, 2014.

• Elodie Leducq, *Autour des codes de Reed-Muller généralisés*, Paris 7, 2011.

Robert Rolland :

• Julia Pieltant, Marseille, 2012.

• Milakulo Tukumuli, Marseille, 2013.

• Kevin Atighehchi, Maresille, 2015.

• Marco Calderini, 2015, rapporteur.

Diffusion de la recherche : Colloques

a) Comités scientifiques (ou de programme)

Yves Aubry :
• Comité de programme de WCC'2011 (The Seventh International Workshop on Coding and Cryptography 2011) qui s'est tenu à l'IHP (Institut Henri Poincaré) à Paris du 11 au 15 avril 2011.

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

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

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

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

Gilles Lachaud :
• Co-leader, group 6, Workshop "Algebraic Geometry for Coding Theory and Cryptography", Institute for Pure & Applied Mathematics (NSF – UC Los Angeles), 22-26 février 2016.

David Kohel :
• YACC 2016.
• ANTS 2016.

François Rodier :
• Colloque international CAI 2013
• Geocrypt 2013
• YACC 2012

b) Comités d'organisation

Yves Aubry :
• The 15-th AGC^2T conference (Arithmetic, Geometry, Cryptography and Coding Theory), CIRM, 19-23 juin 2017, co-organisateur.
• Colloque YACC'2016 (Yet Another Conference in Cryptography) - Colloque international en cryptographie - Porquerolles 06-10 juin 2016. Organisateur principal.
• Dixièmes Journées Scientifiques de l'Université de Toulon - 26-27 avril 2016 : Codes géométriques et algébriques. Organisateur principal.
• Neuvièmes Journées Scientifiques de l'Université de Toulon - 21-22 avril 2015 : Information quantique et sécurité de l'information (QUBIT). Organisateur principal.
• Colloque YACC'2014 (Yet Another Conference in Cryptography) - - Colloque international en cryptographie - Porquerolles 09-13 juin 2014. Organisateur principal.
• Colloque YACC'2012 (Yet Another Conference in Cryptography) - - Colloque international en cryptographie - Porquerolles 24-28 septembre 2012. Organisateur principal.
• The 13-th AGC^2T conference (Arithmetic, Geometry, Cryptography and Coding Theory), CIRM, 14-18 mars 2011, co-organisateur.
• Colloque international GeoCrypt'2011 et GeoCrypt'2013.

Stéphane Ballet et Alexis Bonnecaze :
• Membre du Comité d'organisation de la Journée sécurité AMUSEC, Rencontre annuelle des acteurs de la sécurité des systèmes d'information de la région PACA à Polytech Marseille, Luminy, le 24 mars 2016.

Stéphane Ballet :
• Membre du Comité d'organisation du colloque international AGC^2T14 "Arithmetic, Geometry, Cryptography and Coding Theory", CIRM, juin 2013.

David Kohel :

• Coordination du mois thematique *Arithmétique* dans le cadre du programme de la Chaire Morlet (Igor Shparlinski) (colloques *Unlikely Intersections* (3–7 février), *Prime Numbers : New Perspectives* (10–14 février), *Frobenius Distributions on Curves* (école 17–21 février, et colloque 24–28 février), *On the conjectures of Lang and Vojta* (3–7 mars)), 2014.

• Organisation de l'École d'hiver et colloque *Frobenius Distributions on Curves*, 17-28 février 2014, avec Igor Shparlinski et Christophe Ritzenthaler.

• Arithmétique, Géométrie, Cryptographie et Théorie des Codes, 18–22 mai, 2015, avec Alp Bassa et Alain Courvreur.

Christophe Ritzenthaler :

• Membre du Comité d'organisation de Geocrypt-2 à Furiani du 20 au 24 juin 2011.

• Membre du Comité d'organisation de AGC2T-13 au CIRM du 14 au 18 mars 2011.

Robert Rolland :

• Organisation de la Conference on Algebraic Informatics (CAI 2013) avec proceedings dans LNCS 8080.

• Organisation de l'International Symposium on Parallel and Distributed Computing (ISPDC 2014) avec proceedings publiés par IEEE.

Diffusion de la recherche

Gilles Lachaud a donné 3 exposés de diffusion de la recherche :

• Assemblée Générale de l'IREM (Marseille).
Conférence : *Actualité de Diophante*. 4 mai 2011.

• Cycle de Conférences "Les Horizons du Savoir", ASTS (Marseille).
Conférence : *Mathématiques et Communication : d'Alexandrie à San Francisco*. 7 février 2012.

• Les Jeudis du CNRS (Marseille).
Conférence : *Transmission de données : codage, décodage*. 3 mai 2012.

Formation par la recherche :

• Accueil de Samrith Ram sur un contrat post-doctoral du Labex Archimède, du 1er mars 2013 au 30 juin 2014.

Projets et collaborations

Projet international

• Stéphane Louboutin est membre du Projet Franco/Japonais *Zeta Functions of several variables and applications* piloté par D. Essouabri (Saint Etienne) et K. Matsumoto (Nagoya), débutant le 01/04/2015, se terminant le 31/03/2017 et financé par la Japan Society for the Promotion of Science (JSPS) et le Centre National de la Recherche Scientifique (CNRS). Lien : https ://sites.google.com/site/fjzeta2015/home

Missions de recherche

a) Missions nationales :

• Yves Aubry collabore avec Marc Perret de l'université de Toulouse (Institut de Mathématiques de Toulouse) sur l'étude des codes géométriques algébriques en dimansion supérieure, à savoir sur des variétés algébriques de dimension au moins 2. Il donne lieu à des échange d'invitations.

De plus, une retraite de l'ANR Manta est programmée du 11 au 15 avril 2016 dans le village Lacapelle Biron (47150, Lot et Garonne).

• Stéphane Ballet a été invité

- Dans le Groupe Mathématiques de l'Information, des Communications et du Calcul (MIC2) du Laboratoire Communications et Traitement de l'Information (LCTI) au sein du Département Informatique et

Réseaux (INFRES), Telecom ParisTech, Paris, Convention de séjour sabbatique du 15 juin au 10 juillet 2015 (1 mois).

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

- A l'UPF, Laboratoire GAATI en Polynésie Française : Novembre 2012 (1 mois).

• Christophe Ritzenthaler a été invité par R. Lercier à l'IRMAR de Rennes en avril et janvier 2011.

• François Rodier a été à l'université de Polynésie Française où il a donné un exposé *Highly resistant Boolean Functions for Cryptography*.

b) Missions internationales :

• L'institut de Mathématiques Pures et Appliquées (Institut for Pure and Applied Mathematics (IPAM)) de l'Université de Californie à Los Angeles (University of California Los Angeles (UCLA), USA), a organisé du 22 au 26 février 2016 un workshop intitulé "Algebraic geometry for coding theory and cryptography". Yves Aubry a été invité à faire partie du groupe de travail *Number of points of algebraic sets* qui a pour but d'étudier et de généraliser la borne de Serre concernant le nombre de points maximal d'une hypersurface projective qui avait été conjecturée par Tsfasman.

Ce groupe de travail est constitué des chercheurs suivants : Yves Aubry, Wouter Castryck, Sudhir Ghorpade, Gilles Lachaud, Mike O'Sullivan et Samrith Ram, chercheurs respectivement à Ghent (Belgique), Bombay (Inde), Marseille (France), San Diego (USA) et Bombay (Inde).

• Stéphane Ballet a été invité à l'Université Indépendante de Moscou, Unité Mixte Internationale Poncelet, à Moscou (Russie) : invitation par le professeur Michaël Tsfasman, septembre 2013 pour le semestre thématique Global Field.

• François Rodier a été invité à la conférence *Algebraic geometry and number theory* au laboratoire Poncelet à Moscou du 23 au 27 juin 2014.

• Serge Vladut a été invité par Grigory Kabatiansky (Institute for Information Transmission Problems, Moscow) de septembre 2014 à décembre 2014. Collaboration sur le thème de "compressed sensing" pour les codes correcteurs d'erreurs sur un corps fini.

Activités Administratives

Yves Aubry a été de 2011 à 2013 vice-président de la Société Mathématiques de France (SMF), membre du bureau de la SMF (site I.H.P. à Paris), membre du Conseil d'Administration de la SMF (site I.H.P. à Paris), responsable de la Maison de la SMF (site à Luminy), et membre-invité du Conseil d'Administration du CIRM.

Par ailleurs, les membres d'ATI ont participé à plus d'une dizaine de comités de sélection. Ils ont aussi participé à 3 ANR différentes.

Gestion d'ANR :

• ANR MANTA (2016–2019) (Y. Aubry)
• ANR CHIC (2009–2012) (D. Kohel, C. Ritzenthaler)
• ANR PEACE (2012–2015) (D. Kohel, C. Ritzenthaler)

Mission d'expertise :

• Yves Aubry est membre de l'Editorial board de la revue internationale : *International Journal of Information and Coding Theory*.

• Gilles Lachaud a effectué une mission d'expertise pour la société $\mathbb{Z}_2$-Innovation (Paris La Défense), 2012.

• Gilles Lachaud est Rapporteur pour les Comptes-Rendus de l'Académie des Sciences.

• Alexis Bonnecaze a effectué une mission d'expertise pour la revue finale de projets du programme ANR Programme Contenus numériques et interactions 2011 et pour la revue finale de projets du programme "ANR TELECOM 2007", en 2012.

1.3.3 Interaction avec l'environnement social, économique et culturel

L'équipe ATI est très ouverte au monde non scientifique et interagit avec différents acteurs, académique, grand public et industriel. Annamaria Iezzi, doctorante, s'investit beaucoup dans la diffusion du savoir vis-à-vis des jeunes et du grand public et dans la vulgarisation des mathématiques (exposés pour Maths en Jeans, Fête de la Science, Ecole de la deuxième chance, stages hypocampes). Elle prend une part active à l'organisation de la journée de Pi à Marseille (http ://www.piday.fr/). Elle est récipiendaire du prix d'Alembert 2016 de la société mathématique de France (Ce prix vise à encourager la diffusion de la connaissance des mathématiques vers un large public). Stéphane Ballet et Alexis Bonnecaze ont aussi donné des exposés à des lycéens pour faire connaitre les domaines des mathématiques et de la cryptographie.

L'équipe ATI cherche à se faire connaitre des entreprises afin d'offrir à celles-ci des services d'expertises pouvant se traduire par des contrats industriels. En 2011, Alexis Bonnecaze et Robert Rolland ont obtenu un contrat (30 KE) avec l'entreprise IMS consistant a proposer un mécanisme cryptographique pour assurer l'anonymat de données collectées. La proposition a été acceptée par la CNIL et déployée sur plusieurs milliers de pharmacies. Ce travail a aussi donné lieu a une présentation à la conférence YACC 2014.

C'est dans ce même esprit que la 14eme rencontre Math-industrie à l'ESIL le 16 juin 2011 (Nombre et hasard, avec le soutien de la SMAI, SMF, INRIA, CNRS et FRUMAM. http ://mathindustrie14.sciencesconf.org/.) et la journée Sécurité AMUSEC à Polytech-Marseille le 24 Mars 2016 (avec le soutien du LabEx Archimède et du Clusir-Paca, http ://amusec.sciencesconf.org/) ont été organisées.

Alexis Bonnecaze est par ailleurs correspondant du Clusir-Paca à Polytech-Marseille.

1.4 Implication de l'équipe dans la formation par la recherche

L'école doctorale concernée est celle de mathématiques et informatique (ED184).

L'équipe s'implique dans plusieurs masters (mathématiques, mathématiques discrètes et fondements de l'informatique (MDFI), mathématiques de l'université du sud Toulon-Var) en enseignant dans ces masters ou en l'organisant (MDFI). Plus de 10 stages de Masters ont été encadrés.

1.5 Stratégie et perspectives scientifiques pour le futur contrat

Le projet scientifique d'ATI se poursuit dans la continuité avec certaines directions qui ont été décrites dans la section Production scientifique. Au niveau stratégique, ATI s'attachera à

- renforcer les collaborations transdisciplinaires en mettant les mathématiques de sa spécialité au service d'autres disciplines et à renforcer sa collaboration avec des laboratoires de disciplines connexes (en particulier l'informatique).
- Développer la dimension R&D de son activité en coopération avec les entreprises du tissu économique local.
- Ces dernières années, l'équipe ATI a connu une très forte baisse de ses effectifs avec le départ de 5 permanents reconnus internationalement dans le domaine de spécialité susmentionné : le départ de Michel Laurent (DR CNRS), les départs à la retraite de Gilles Lachaud (DR CNRS émérite), François Rodier (DR CNRS émérite), Robert Rolland (MCF émérite), ainsi que la nomination au poste de Professeur des Universités de Christophe Ritzenthaler à l'Université de Rennes I. Ces départs n'ont été compensés par aucune arrivée.

L'équipe continue d'avoir une production scientifique importante (une centaine de publications durant la période) et de qualité mais cette baisse des effectifs a pour conséquence un ralentissement naturel de son implication dans certains projets en cours, l'impossibilité mécanique d'honorer des demandes concernant de nouveaux projets (coopérations interdisciplinaires, coopération avec des entreprises locales, vulgarisation et communication etc...) ainsi que l'incapacité à candidater à divers projets (ANR, etc).

Pour ces raisons, l'équipe a impérativement besoin de recruter un chercheur (MC ou PR) sur un poste en interaction mathématiques-informatique dans le domaine de spécialité de la théorie algorithmique des nombres ayant un potentiel d'application à la cryptologie ou plus généralement à la théorie de l'information. Ce recrutement permettrait de retrouver l'équilibre que l'équipe avait avant ces départs. L'objectif est de rétablir une masse critique permettant à la thématique de survivre.