INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

PROJET CODES

Codage et cryptographie

Rocquencourt

THÈME 2B

Table des matières

1 Composition de l'équipe

Responsable scientifique

Pascale Charpin [DR, INRIA]

Responsable permanent

Nicolas Sendrier [CR, INRIA]

Assistante de projet

Christelle Guiziou-Cloitre

Personnel INRIA

Daniel Augot [CR]

Anne Canteaut [CR]

Conseiller scientifique

Guy Chassé [École des Mines de Nantes]

Collaborateurs extérieurs

Thierry Berger [Université Limoges]

Francis Blanchet [Lycée Montaigne]

Claude Carlet [Université Caen]

Caroline Fontaine [Université Lille]

Sami Harari [Université de Toulon]

François Laubie [Université Limoges]

Dominique Le Brigand [Université Paris 6]

Chercheur Invité

Simon Litsyn [Université de Tel Aviv, Israël, de juillet à novembre 1999]

Chercheurs doctorants

Matthieu Brunet [X-Telecom, CNET, depuis septembre 1999]

Éric Filiol [Ministère de la Défense, depuis octobre 1997]

Pierre Loidreau [Ingénieur de l'Armement, Ministère de la Défense, depuis octobre 1997]

Lancelot Pecquet [Bourse INRIA, depuis octobre 1997]

Gintaras Skersys [Bourse Régional, Université de Limoges, depuis janvier 1997]

Antoine Valembois [Bourse DGA, depuis septembre 1997]

Djessy Vianne [Ministère de la Défense, depuis septembre 1999]

Stagiaires

Hervé Alavoine [Stage de fin d'Études, I.U.T. Villetaneuse, Université de Paris 13, d'avril à juin 1999]

Stéphane Cutajar [Stage de fin d'Études, École Spéciale Militaire de Saint-Cyr/Écoles de Coëtquidan, de mars à mai 1999]

Christophe Libert [Stage de fin d'Études, École Spéciale Militaire de Saint-Cyr/Écoles de Coëtquidan, de mars à mai 1999]

Grégory Olocco [Stage de DEA, Université de Paris 7, d'avril à juin 1999]

Ayoub Otmani [Stage de DEA, Université de Limoges, d'avril à juin 1999]

Christine Pourcelot [Stage d'Ingénieur, C.N.A.M., d'octobre 1998 à octobre 1999]

Michaël Trabbia [Stage de fin d'Études, École Polytechnique, d'avril à juillet 1999]

2 Présentation et objectifs généraux

Le domaine de recherche du projet *CODES* est centré sur l'étude de la *Protection de l'Information* numérique. Le contexte est *large*, prenant en compte l'évolution de la théorie algébrique des codes et des techniques de codage, ainsi que l'apparition de nouvelles applications. On peut donner deux exemples qui illustrent les deux principaux aspects des activités du projet.

D'une part, le projet s'investit dans l'étude de la construction effective et des performances des *codes géométriques* (et de leurs dérivés). Il est clair en effet que la communauté scientifique considère que ces codes sont porteurs d'applications futures. Et ceci, non seulement à cause de leurs hautes performances, mais parce qu'ils contribuent au développement des outils géométriques pour le traitement de l'information.

D'autre part, le projet s'investit dans un ensemble de problèmes relevant de la *confidentialité* de l'information. Et cet investissement se traduit tant au niveau de la recherche fondamentale que dans le choix d'applications précises telles celles liées à la transmission des images.

Ce choix délibéré, de traiter une théorie, dans ses aspects *mathématiques* et *informatiques*, et ses applications, a enfin pour motivation fondamentale la formation par la recherche. Il convient, en effet, par l'environnement créé au projet, de répondre à une demande. Le profil dessiné serait : double compétence, mathématique et informatique, dans le domaine du codage. À titre d'exemple, ce profil est demandé actuellement pour concevoir et mettre en œuvre les algorithmes intervenant dans les cartes à puces.

3 Fondements scientifiques

Le codage en général relève de la théorie de l'information. La correction d'erreurs et le chiffrement sont des aspects importants de la protection de l'information. Il s'agit d'une part de résister au *bruit* et d'autre part de lutter contre les *fraudes*. Ces deux démarches contradictoires, *révéler* contre *cacher*, sont souvent complémentaires.

La *théorie algébrique des codes* s'est développée à partir des problèmes posés par la résistance au bruit ; les codes correcteurs doivent protéger une information transitant à travers un canal de transmission soumis à des perturbations. Ce canal peut être une ligne téléphonique, une liaison radio ou encore un support magnétique ou optique : bande magnétique ou disque compact. Le codage consiste en l'ajout d'une redondance, et le décodage doit permettre, à partir de la sortie codée puis perturbée du canal, de restituer de façon acceptable l'information fournie par la source.

Depuis les premiers codes de HAMMING et surtout la découverte des fameux codes BCH (1960), la théorie algébrique des codes correcteurs connaît un développement constant, elle est devenue centrale en tant qu'application des mathématiques discrètes. Le dynamisme de la discipline peut se mesurer par le nombre et la qualité des colloques qui lui sont consacrés et où se mèlent des travaux autant théoriques qu'appliqués utilisant tous les outils des mathématiques discrètes (algèbre des structures finies, combinatoire, géométries finies...) ainsi que ceux, plus modernes, de l'informatique théorique, notamment l'algorithmique et le calcul formel.

De même que les mathématiques ont pu apporter énormément aux codes correcteurs d'erreurs en établissant ses fondements théoriques, les objets ayant les propriétés les plus intéressantes en cryptographie, et notamment en cryptographie à clé publique, proviennent des mathématiques ; le système de chiffrement RSA, le protocole d'échange de clé de Diffie-Hellman ou encore les plus récentes utilisations des courbes elliptiques, se fondent en grande partie sur la théorie algébrique des nombres. Aujourd'hui, d'autres cryptosystèmes à clé publique (McEliece, Niederreitter, Gabidulin, Sidelnikov, ...) reposent sur la théorie des codes correcteurs d'erreurs. Depuis quelques années, ce sont la théorie des codes et les mathématiques discrètes qui apportent à la cryptographie[1] dans des problèmes tels que le partage du secret, la conception de cryptosystèmes symétriques résistant aux cryptanalyses par corrélation, différentielles ou linéaires, le marquage d'images pour la protection des droits d'auteur, ... Des problèmes

1. J.L. MASSEY – Some applications of coding theory in cryptography. *In : Codes and Cyphers: Cryptography and Coding IV*, éd. par Farell (P.G.). pp. 33–47 – Springer-Verlag

de recherche revêtant une grande importance pour les applications dans le domaine des télécommunications apparaissent qui justifient le développement d'une communauté possédant une palette large de compétences. Ceci apparaît dans les activités d'un nombre croissant de laboratoires de recherche dans le monde. Une étude récente de la NSF Américaine[2] montre aussi la reconnaissance d'un nouveau domaine de recherche ainsi qu'une volonté institutionnelle de coordonner les efforts.

Notre projet se positionne nettement dans le contexte décrit plus haut; nos thèmes de recherche sont actuellement :

1. Étude et analyse de structures discrètes;
2. Cryptographie à clé publique (systèmes basés sur les codes, sur les courbes);
3. Primitives du chiffrement symétrique (fonctions booléennes, séquences, polynômes ...);
4. Algorithmes de décodage (correction d'erreurs et cryptanalyse);
5. Protection des droits d'auteurs (watermarking).

4 Résultats nouveaux

4.1 Étude et analyse de structures discrètes

Les chercheurs du projet s'intéressent aux propriétés générales structurelles des codes, dans un espace ambiant donné. Il s'agit d'un sujet théorique *en amont* qui a pour but essentiellement de classifier un ensemble d'objets prédéfinis. L'ensemble de ces travaux constitue une base théorique fondamentale pour les actions finalisées décrites plus loin. Il s'agit de caractériser des classes d'objets exceptionnels, de concevoir des outils pour les traiter, de reconnaître une structure ...

4.1.1 Groupes d'automorphismes

Participants : Thierry Berger, Pascale Charpin.

Reconnaître deux codes équivalents, reconnaître un code destructuré par permutations, accélérer certaines procédures de décodage, tous ces problèmes relèvent de l'étude des automorphismes des codes – i.e. des transformations isométriques conservant le code. Les chercheurs du projet ont obtenu des résultats importants dans ce domaine. Les plus marquants sont : la détermination du groupe de permutations des codes BCH primitifs et un nouvel algorithme de preuve de l'équivalence de deux codes linéaires binaires.

Utilisant les travaux de Delsarte (1969) et l'approche combinatoire des codes affine-invariants, due à P. Charpin (1987), T. Berger et P. Charpin ont pu mettre en place une série d'outils, algorithmiques ou combinatoires, permettant de déterminer effectivement les groupes de permutations. Ce travail, qui donne comme principale application le groupe de permutations des codes BCH primitifs, a été présenté dans plusieurs colloques internationaux. Un article complet

2. National Science Foundation. – *Report of the Working Group on Cryptology and Coding Theory*, avril 1997

est paru fin 1996 sous forme de *regular paper* dans IEEE Transactions on Information Theory [2] . Les groupes d'automorphismes des codes BCH, définis sur une extension de corps, sont décrits dans [15].

D'autre part, T. Berger s'est intéressé aux groupes d'automorphismes des codes *alternants*. Ces codes sont des sous-codes des codes de Reed-Solomon généralisés et contiennent les codes de Goppa classiques. Il a montré qu'il existe quatre classes de codes alternants cycliques et que parmi ceux-ci certains sont des codes de Goppa [34].

4.1.2 Codes équivalents.

Participants : Gintaras Skersys, Nicolas Sendrier.

Deux codes sont équivalents par permutation s'il existe une permutation des coordonnées de l'un le transformant en l'autre. Le problème de décision associé a été étudié récemment par Petrank et Roth[3] qui ont montré qu'il n'était pas NP-complet, mais était, en revanche, au moins aussi dur que le problème de décider de l'équivalence entre deux graphes. Trouver un algorithme efficace pour résoudre le problème de l'équivalence des codes présente donc un intérêt certain.

N. Sendrier a conçu et mis en œuvre un nouvel algorithme, permettant de tester l'équivalence de deux codes linéaires donnés. Cet algorithme est capable de décider, dans presque tous les cas, de l'équivalence (par permutation) de deux codes à partir d'un invariant (*i.e.* une propriété d'un code invariante par permutation du support). Cet invariant devra pouvoir se calculer en temps polynomial, et devra être discriminant, c'est-à-dire prendre *souvent* des valeurs distinctes pour deux codes non équivalents. La difficulté consiste à faire fonctionner l'algorithme lorsque *souvent* n'est pas très proche de *tout le temps* (par exemple une fois sur deux).

Cet algorithme, dit *algorithme de séparation du support (support splitting algorithm)* utilise les invariants du *Hull* – i.e. intersection d'un code avec son dual. L'énumérateur des poids du Hull d'un code est un invariant facile à calculer sauf pour une proportion exponentiellement faible de codes et fournit une discrimination suffisante pour décider de l'équivalence de deux codes et pour retrouver la valeur de la permutation.

Un article, décrivant cet algorithme dans un cadre plus général vient d'être accepté ; il s'agit d'un *regular paper* à IEEE-IT [30] (voir aussi [53]). Les diverses applications possibles de l'algorithme, en relation avec la solidité de certains cryptosystèmes sont présentées dans §4.2.1.

Dans le cadre de sa thèse, G. Skersys a étudié avec N. Sendrier les algorithmes de calcul des groupes d'automorphisme des codes linéaires. Il a obtenu des améliorations importantes des algorithmes connus dans ce domaine [51, 72].

G. Skersys a soutenu sa thèse en Octobre 99. Il y présente, en outre, une étude précise du Hull des codes cycliques [12].

3. E. Petrank and R.M. Roth, *Is code equivalence easy to decide?* IEEE Transactions on Information Theory, 43 (5), pp. 1602–1604, septembre 1997.

4.1.3 Codes de Goppa

Participants : Thierry Berger, Francis Blanchet, Grégoire Bommier, Pierre Loidreau.

Les codes de Goppa binaires sont souvent dits *quasi-aléatoires* — i.e. très "proches" des codes aléatoires. On dispose d'un algorithme efficace de décodage des codes de Goppa. C'est pour ces raisons qu'ils sont utilisés dans certains cryptosystèmes et qu'ils assurent une meilleure sécurité pour les transmissions par un canal bruité. D'autre part leurs propriétés, combinatoires ou algébriques, sont liées aux propriétés générales des polynômes sur les corps finis (en caractéristique 2), et ceci de façon plus évidente que pour n'importe quels autres codes.

Les familles de codes décrites ci-après constituent des classes de clés faibles du cryptosystème de McEliece (voir §4.2.1).

T. Berger a effectué une étude extrêmement fine des groupes de permutations des codes de Goppa afin d'identifier des structures particulières. Ses résultats sont importants, prolongeant notamment les travaux de H. Stichtenoth[4]. Il obtient de nouvelles familles de codes de Goppa cycliques ou d'extension cyclique. Il exhibe des codes de Goppa non cycliques dont le sous-code de poids pair est cyclique. Beaucoup parmi eux sont quasi-cycliques et ont des paramètres inconnus pour des codes quasi-cycliques. Certains atteignent les meilleures bornes connues pour des codes linéaires (voir [16, 17, 34, 60]).

P. Loidreau a construit des nouvelles familles de codes dérivés de codes de Goppa possédant certains invariants. Des bornes en distance et en dimension des codes de Goppa, on peut déduire des bornes en distance et en dimension des codes dérivés [48, 68].

L'intérêt de cette nouvelle famille de codes est de représenter presque parfaitement les codes de Goppa dont ils sont issus, tout en étant de longueur et de dimension bien plus petites.

F. Blanchet et G. Bommier ont démontré que certaines contraintes explicites sur les paramètres, induisent la *quasi-cyclicité* d'un code de Goppa [18].

4.1.4 Codes sur un module de type $\mathbf{Z}/p\mathbf{Z}$

Participant : Claude Carlet.

L'introduction par Hammons et al. (1993) de la notion de code $\mathbf{Z}_4$-linéaire a ouvert un pan complet de recherche dans le domaine des codes correcteurs d'erreurs. Il n'existait pas jusqu'à présent de généralisation de cette notion à celle de code $\mathbf{Z}_{2^k}$-linéaire. C. Carlet a introduit récemment une telle généralisation. Il en a déduit de nouveaux codes, qui généralisent les codes de Kerdock et de Delsarte-Goethals [24].

C. Carlet a également caractérisé les codes $\mathbf{Z}_4$-linéaires dont les mots non nuls sont tous de même poids et établi une borne supérieure et une borne inférieure sur leur distance au code de Reed-Muller d'ordre 1. Cette distance joue un rôle important en cryptographie [40].

Enfin, il a poursuivi l'étude des codes de Kerdock du point de vue de leur $\mathbf{Z}_4$-linéarité [41].

4. H. Stichtenoth, *Which extended Goppa codes are cyclic?*, Journal of Combinatorial Theory, series A 51, pp. 205-220, 1989.

4.1.5 Codes lexicographiques

Participant : François Laubie.

F. Laubie poursuit l'étude des codes lexicographiques, codes produits itérativement à partir d'un alphabet donné. Dans [65], il construit des codes de type *Greedy* qui sont naturellement linéaires, quelle que soit la caractéristique du corps constituant l'alphabet.

4.1.6 Codes cycliques et trinômes sur un corps fini

Participants : Pascale Charpin, Pierre Loidreau.

P. Charpin, en collaboration avec A. Tietäväinen (université de Turku) et V. Zinoviev (IPPI, Académie des Sciences de Moscou) s'intéresse aux codes cycliques de grande dimension. Il s'agit de jeter les bases d'une classification des codes engendrés par deux polynômes minimaux. Les objets étudiés sont fondamentaux, apparaissant dans de nombreuses applications où interviennent des séquences, des fonctions booléennes ou bien dans la problématique du *logarithme discret*. L'article le plus récent traite des codes définis sur des corps de caractéristique impaire [26].

Les problèmes abordés ici relèvent de la théorie des corps finis. Précisément la détermination des mots de petit poids des codes étudiés est obtenue en factorisant des classes de polynômes lacunaires. Il s'agit notamment de *trinômes*. Dans ce contexte, P. Loidreau a étudié les trinômes ternaires. Il a introduit des conditions d'existence de trinômes, sur le corps d'ordre 3, irréductibles et primitifs [49].

L'étude des codes cycliques primitifs est étroitement liée à l'étude de certaines suites binaires ou encore des permutations utilisées dans le chiffrement par blocs. Les travaux des chercheurs du projet sur ce thème, notamment les résultats récents de A. Canteaut et P. Charpin, sont décrits plus loin, §4.4.

4.1.7 Théorie des nombres, algèbre finie

Participants : François Laubie, Dominique Le Brigand.

F. Laubie a montré que l'addition des entiers en base p sans retenue est récursive [29]. Ce résultat n'était connu que pour $p = 2$ ou 3.

F. Laubie étudie d'autre part les groupes de Lie p-adiques compacts qui sont des groupes de Galois locaux. Étant donné un groupe de Lie p-adique G et une extension finie K du corps des nombres p-adiques, il a montré qu'il n'existe qu'un nombre fini de filtrations de G susceptibles d'être les filtrations de ramification des extensions totalement ramifiées de K, de groupe de Galois G [28].

Pour les corps de nombres, E. Brown et C. J. Parry ont déterminé toutes les extensions bicycliques biquadratiques imaginaires dont l'anneau des entiers est principal. Avec Y. Aubry (Université de Caen), D. Le Brigand a résolu le problème analogue pour les corps de fonctions dans le cas de la caractéristique 2 (le cas de caractéristique impaire avait été fait par X.-K. Zhang précédemment) [13].

4.2 Cryptographie à clé publique

4.2.1 Système utilisant des codes correcteurs

Participants : Anne Canteaut, Pierre Loidreau, Nicolas Sendrier, Antoine Valembois.

Dans ce thème, sont regroupés l'étude et la conception de systèmes de protection de l'information où interviennent des codes correcteurs. Les clés utilisées sont en général publiques. Ces systèmes sont fondés sur des problèmes *durs* de théorie des codes, essentiellement décoder et/ou identifier un code dont la structure ou les paramètres sont cachés.

L'étude des *codes permutés* est un aspect de la recherche sur les systèmes basés sur les codes correcteurs. Il s'agit de savoir dans quelle mesure l'action d'une permutation détruit la structure d'un code donné. C'est en ce sens que les travaux sur les codes équivalents ont des applications en cryptographie (cf. §4.1.1, §4.1.2 et §4.1.3). Cette attaque, dite *attaque par structure*, permettrait de retrouver la clé secrète d'un cryptosystème de type McEliece. Dans un domaine plus théorique, il s'agit de déterminer des classes de clés (i.e. de codes) *faibles*.

N. Sendrier a montré que les *codes concaténés* du premier ordre ne sont pas fiables lorsqu'on les utilise dans des cryptosystèmes à clé publique de type McEliece ou Niedereitter. En effet, la forme très particulière des mots de petit poids du dual des codes concaténés permet de retrouver la structure concaténée pourtant cachée par une permutation aléatoire [31].

Jusqu'à ce jour, il n'y avait pas de résultat connu sur l'attaque par structure du système de McEliece basé sur les codes de Goppa. La structure des codes de Goppa semble suffisamment complexe, la classe suffisamment large. Dans ce contexte, P. Loidreau et N. Sendrier ont réalisé une avancée importante en isolant des classes de codes de Goppa qui possèdent certains invariants, des isomorphismes de corps. Il s'agit d'une application remarquable de l'algorithme de *séparation du support* de N. Sendrier (cf. §4.1.2). Une étude précise des invariants utilisés avait été réalisée par P. Loidreau pour son mémoire de DEA, et ceci aboutit à la mise en évidence de clés faibles dès que l'on veut cacher un ensemble de messages avec des codes de Goppa [67].

D'autre part, A. Canteaut et N. Sendrier se sont intéressés à l'implémentation des cryptosystèmes à clé publique basés sur les codes correcteurs. Des éléments nouveaux permettant d'optimiser le choix des paramètres ont été présentés au colloque de cryptologie ASIACRYPT'98 [36].

A. Valembois étudie, dans le cadre de sa thèse, les diverses procédures d'identification de codes linéaires. Le problème est, disposant d'un train binaire constitué de blocs de même longueur (les mots de code), de reconstituer le code utilisé [54, 55, 74]. A. Valembois a dirigé le stage de S. Cutajar et C. Libert (stage de fin d'École, Coëtquidan) pour réaliser un simulateur de transmissions numériques bruitées [61].

4.2.2 Courbes elliptiques

Participant : Daniel Augot.

Ces dernières années, l'évolution des logiciels de calcul formel et le développement du thème *Géométrie algébrique et codage*, ont amené les chercheurs à formuler d'importants problèmes de recherche en terme de résolution de systèmes d'équations sur les corps finis. Il en est ainsi pour

la détermination de mots de poids faible pour certains codes correcteurs. Dans le même temps s'est développée la cryptologie basée sur les courbes elliptiques, proposant une technologie globalement plus efficace que RSA.

Sur ces thèmes, nous nous situons plutôt en algorithmique. Nous nous intéressons d'abord à concevoir ou étudier des algorithmes (implémentations, complexité, programmation de fonctionnelles issues de la géométrie algébrique ...).

L'activité principale cette année a été le lancement de l'*action de recherche coopérative* (ARC) "COURBES" dirigée par Daniel Augot[5]. Elle regroupe trois équipes ayant des compétences complémentaires : le projet CODES, le LIX (École polytechnique) et le LACO (Université de Limoges). Les deux principaux axes de recherche sont :

- Analyse des courbes elliptiques et hyperelliptiques – cryptanalyse des systèmes existants.
- Recherche et étude de nouvelles courbes – conception et optimisation de cryptosystèmes.

Daniel Augot a présenté la problématique des courbes elliptiques en cryptologie à la 27e École de printemps d'informatique théorique [33] – Batz-sur-mer, Juin 99.

4.3 Algorithmes de décodage et cryptanalyse

Participants : Daniel Augot, Lancelot Pecquet, Anne Canteaut, Gregory Olocco, Ayoub Otmani, Michaël Trabbia.

Le décodage des codes en bloc connaît un regain d'intérêt et ceci pour deux raisons. La première est la persistance de problèmes ouverts liés à la conception et à l'amélioration d'algorithmes spécifiques – pour décoder des codes performants tels les codes *géométriques* ou les codes *résidus quadratiques*. La deuxième est l'apparition de nouvelles applications en correction d'erreurs et en cryptologie.

L'étude des performances des *petits codes correcteurs en bloc* est d'actualité à cause du développement de systèmes où l'information est transmise *par paquets* de petites longueurs. Le but recherché actuellement est de concevoir des systèmes où la rapidité avoisinerait celle obtenue lorsque l'on effectue une correction en ligne. Nous avons commencé cette année à développer ce thème de recherche par l'étude de nouveaux codes, dits *codes CORTEX*. Ces codes sont construits à partir d'un ensemble de codes de longueur 8 ou 4, concaténés et entrelacés. Les codes CORTEX sont autoduaux. Leur structure est étudiée dans [70] et leurs performances dans [69] par, respectivement, A. Otmani et G. Olocco (stagiaires dirigés par P. Charpin et J.P. Tillich – LRI, Orsay).

Lancelot Pecquet étudie, pour sa thèse, l'algorithme de Sudan. Cet algorithme, dit *de décodage par liste*, suscite un vif intérêt dans la communauté du codage, car il présente un paradigme nouveau pour décoder. Il s'agit d'un décodage par interpolation plutôt que par calcul de syndromes. Un premier résultat, obtenu par D. Augot et L. Pecquet est un gain considérable sur la complexité de l'algorithme. Essentiellement, une méthode de factorisation à deux variables sur les corps finis est remplacée par une itération de Newton [59]. Une version

5. www-rocq.inria.fr/codes/Daniel.Augot/courbes

plus générale de cette méthode a été présentée par L. Pecquet au colloque international "Finite Fields and Applications" [50].

Suite à de nombreux travaux récents, il est bien connu que les algorithmes de décodage sont des outils performants en cryptanalyse. Le projet s'est investi depuis longtemps dans ce domaine de recherche[6] et un certain nombre de sujets ont été abordés cette année.

Ainsi l'*attaque par décodage des systèmes de chiffrement par flot* est le sujet du rapport de stage de M. Trabbia [73] (Polytechnique, stage de fin d'École, direction : A. Canteaut).

4.4 Primitives du chiffrement symétrique

Participants : Anne Canteaut, Claude Carlet, Pascale Charpin, Éric Filiol, Caroline Fontaine.

Dans ce thème, nous voulons étudier et construire des classes de fonctions, polynômes ou séquences qui augmentent la potentialité des systèmes de codage.

Les fonctions booléennes sont utilisées dans de nombreux systèmes de codage. Ils interviennent par exemple dans les protocoles de chiffrement ou dans la définition de séquences *fortement autocorrélées*. Leurs propriétés ont surtout été étudiées par les théoriciens des codes, car elles sont étroitement liées aux propriétés des codes cycliques. Il s'agit là d'un des thèmes de recherche importants du projet, qui contribue à sa reconnaissance dans la communauté internationale en théorie des codes et en cryptologie. Le travail se poursuit depuis plusieurs années tant sur le plan strictement théorique que pour répondre à la demande en *cryptologie*. Cette démarche est précisément décrite par A. Canteaut, dans son exposé pour la 27e École de printemps d'informatique théorique [37].

Haute non-linéarité. Une fonction est de *haute non-linéarité* lorsqu'elle se situe à grande distance de l'espace $R(1,m)$ des fonctions affines de m variables. Cela signifie qu'elle définit un translaté de l'espace $R(1,m)$ de poids de Hamming élevé. La notion de *fonction courbe*, introduite en 1975, désigne la non-linéarité maximum des fonctions booléennes, lorsque m est un nombre pair. Ce maximum est inconnu lorsque m est impair. La classification des fonctions courbes et la détermination de la non-linéarité en dimension impaire, sont des problèmes cruciaux, réputés très difficiles.

C. Fontaine a mené une étude exploratoire de la propriété de non linéarité, s'appuyant sur un corpus de fonctions ayant une représentation courte, correspondant à des mots *idempotents*. Ce corpus, algébriquement très structuré, est aisément manipulable. Les premiers résultats ont montré une bonne distribution des éléments du corpus dans l'ensemble des fonctions booléennes.

L'exploration du corpus des idempotents a permis d'obtenir des fonctions à m variables présentant la meilleure non-linéarité connue pour $m \leq 15$. Certaines possèdent un spectre de Fourier jusqu'alors inconnu, et donnent ainsi de nouvelles distributions des poids pour des translatés du code $R(1,m)$, dont le poids minimum est maximal. Ces nouveaux spectres

6. Un algorithme de décodage aléatoire qui améliore notablement les performances de tous les algorithmes connus précédemment a été réalisé par A. Canteaut. Il s'agissait d'un travail en collaboration avec F. Chabaud (GRECC, ENS-Ulm) [3].

correspondent à des fonctions équilibrées, i.e. dont la sortie est équidistribuée, qui sont de degré élevé. Elles permettent de construire des fonctions présentant de plus un ordre de résilience élevé, qui peuvent être directement utilisées dans certains générateurs pseudo-aléatoires dédiés au chiffrement à flot. Ces résultats ont été présentés à deux conférences internationales dont EUROCRYPT'98 (avec É. Filiol [6]). Un article vient de paraître dans *IEEE Transactions on Information Theory* [27]. C. Fontaine a soutenu sa thèse en Novembre 98 [11].

C. Carlet poursuit un ensemble de travaux sur les fonctions courbes [40, 43]. Il a obtenu avec Ph. Guillot, une caractérisation univoque des fonctions courbes binaires, la forme numérique normale (NNF). Celle-ci permet d'exprimer par des formules explicites le poids et le spectre de Fourier d'une fonction, de caractériser directement les fonctions courbes, de déduire de nouveaux invariants affines sur les fonctions booléennes et d'obtenir des propriétés de divisibilité des poids des fonctions. Ce travail est présenté au colloque AAECC'13 [39].

Les différentes caractérisations existantes des fonctions courbes binaires mènent à des définitions qui, sur l'alphabet Z/qZ, désignent des notions différentes ; on distingue en particulier la famille des fonctions courbes et la sous-famille des fonctions parfaitement nonlinéaires. C. Carlet et S. Dubuc ont montré qu'une seule des constructions connues de fonctions courbes définit des fonctions parfaitement non-linéaires. Ils ont introduit une nouvelle construction qui est la seule connue à ce jour pour des longueurs impaires. Ces résultats sont rassemblés dans un article présenté à *Fifth International Conference on Finite Fields and Applications* [38].

Critère de propagation. La notion de diffusion[7] signifie, dans le cas du chiffrement par blocs par exemple, qu'une faible modification en entrée est diffusée dans l'ensemble du bloc de sortie. C'est un critère de fiabilité en cryptographie, dit critère de propagation pour les fonctions.

Le travail de C. Carlet sur les fonctions hypercourbes se poursuit maintenant dans l'étude et la construction des fonctions qui satisfont le plus généralement les critères de propagation (caractère $PC(\ell)$). Ses premiers résultats constituent un article *invité* dans un volume de *Theoretical Computer Science* dédié à la cryptographie [25].

Fonctions presque courbes, presque parfaitement non-linéaires, et chiffrement à clés secrètes. La cryptanalyse linéaire et la cryptanalyse différentielle sont les principales attaques *connues* des systèmes de chiffrement à clé secrète. Actuellement l'algorithme DES répond à ces impératifs puisqu'aucune technique de cryptanalyse n'est sensiblement plus efficace que l'énumération de toutes les clefs possibles. Toutefois, comme la clef secrète ne comporte que 56 bits, le DES est aujourd'hui extrêmement vulnérable à une recherche exhaustive de la clef. C'est pourquoi un nouvel algorithme de type DES est en cours de standardisation. Pour cela il est nécessaire de remplacer la fonction itérée dans le DES (spécifiée par les boîtes S) par une permutation définie sur un corps fini d'ordre plus élevé ; cette permutation doit de plus vérifier certains critères afin que le système de chiffrement résiste aux attaques classiques.

Dans ce cadre, on utilise des fonctions *presque parfaitement non linéaires* et *presque courbes* car elles assurent une résistance optimale aux cryptanalyses différentielle et linéaire. Ces pro-

7. Définie par C. Shannon dans *Communication theory of secrecy systems*, *Bell system technical journal*, vol. 28, pp. 656-715 (1949).

priétés apparaissent également dans l'étude des suites de longueur maximale puisque les fonctions puissances (i.e. $x \mapsto x^d$) presque courbes coïncident avec des couples de *suites de longueur maximale dont la corrélation croisée est optimale.*

C. Carlet, P. Charpin et V. Zinoviev ont mené une étude fondamentale sur ces fonctions, mettant en évidence les liens avec la classification des codes cycliques de grande dimension. Ceci permet d'utiliser la "boîte à outils" des codes cycliques dans ce contexte. Ce travail a fait l'objet de plusieurs conférences et un article est paru dans *Designs, Codes and Cryptography* [23]. Une étude complémentaire est menée avec A. Tietäväinen (cf. §4.1.6).

Il est montré dans [23] que les fonctions presque courbes correspondent à des codes linéaires dont la distribution des poids est optimale. Dans le cas des fonctions puissances, ces codes sont en fait les duaux de certains codes cycliques à deux zéros. Grâce à cette analogie, A. Canteaut, P. Charpin et H. Dobbertin ont prouvé que les fonctions presque courbes sont entièrement caractérisées par la distance duale et la divisibilité des poids du code qui leur est associée. Ceci leur a notamment permis de démontrer une conjecture formulée par Welch en 1968, selon laquelle la fonction $x \mapsto x^{2^d}$, où $d = (m-1)/2 + 3$, est presque courbe sur $\mathbf{F}_{2^m}$ quand m est impair. Ce résultat est l'objet d'une note à l'académie des sciences de Paris [21] et sera publié dans *IEEE Transactions on Information Theory* [20].

Ce travail a été présenté à *Fast Software Encryption 99* [35]. Un article présentant l'ensemble des résultats obtenus va paraître dans *Siam Journal of Discrete Mathematics* [22].

Fonctions équilibrées. Ce critère signifie qu'une fonction présente en sortie autant de "1" que de "0". É. Filiol étudie les propriétés combinatoires des fonctions booléennes équilibrées. Il s'agit, à partir de la forme algébrique normale d'une fonction booléenne, de détecter la classe de poids (sous-équilibrée, suréquilibrée ou équilibrée) à laquelle elle appartient. Les premiers résultats ont été publiés dans les actes de la conférence Cryptography and Coding [44].

Fonctions t-résilientes. Les fonctions t-résilientes forment une classe de fonctions booléennes très utilisées en cryptographie, en particulier pour l'assemblage des sorties de registres à décalage pour le chiffrement par flot. Elles interviennent également dans la conception de nombreuses primitives conventionnelles telles les fonctions de hachage. P. Camion et A. Canteaut ont établi plusieurs caractérisations générales de ces fonctions en exploitant certaines propriétés de leur transformée de Fourier et leur lien avec les codes correcteurs. Ces travaux leur ont permis de construire de nouvelles classes de fonctions résilientes particulièrement bien adaptées aux applications cryptographiques. La mise à jour, par ce biais, de nouvelles propriétés algébriques des fonctions résilientes et sans corrélation a également conduit à la définition d'un nouveau critère de sécurité pour les primitives cryptographiques conventionnelles [19].

4.5 Protection des droits d'auteurs – watermarking

Participants : Daniel Augot, Mathieu Brunet, Caroline Fontaine.

Le projet a participé, en 1995-98, au projet européen AQUARELLE[8] qui avait pour objet

8. Le réseau d'information sur le patrimoine culturel (Sharing cultural heritage through multimedia tele-

d'homogénéiser les ressources culturelles actuellement existantes (tableaux, manuscrits, photographies ...). Ces ressources appartiennent aux institutions représentées par les différents partenaires culturels. Le but était de présenter à l'usager un système global de découverte et de recouvrement de documents, éventuellement répartis sur des serveurs différents. Dans ce système, les institutions culturelles diffusent des "imagettes" (vignettes) ou des images de moyenne résolution, dont la valeur n'est pas nulle.

Les partenaires culturels ont demandé que soit mise en place une protection de ces images. La solution envisagée repose sur la technique du *filigrane, une "marque" invisible incrustée dans l'image, d'une manière secrète*. Si l'image est utilisée frauduleusement, l'ayant-droit peut attester qu'il est bien propriétaire de l'image.

Du point de vue technique, il s'agit d'un problème de traitement du signal. Une collaboration est établie avec l'équipe TELE, de l'Université Catholique de Louvain (UCL). L'algorithme proposé par UCL est très performant du point de vue de l'invisibilité et de la robustesse à la compression, la contrepartie étant qu'il n'incruste en réalité qu'un seul bit d'information dans l'image (l'image est-elle marquée ou non ?). L'algorithme est paramétré par une clé, dont la connaissance est nécessaire pour vérifier l'existence de la marque.

Le projet CODES a dégagé les fonctionnalités que peut offrir un tel algorithme. Nous proposons de mettre en place un *tiers de confiance* qui sert de serveur de clés et de vérificateur, qui transmet aux propriétaires des images des clés de marquage. Une fois la clé obtenue, le propriétaire peut marquer l'image qu'il souhaite diffuser. En cas de litige, le serveur de clés peut vérifier la présence de la marque, en utilisant la clé correspondante à l'image. Le protocole d'échange de clés repose sur la méthode de Diffie-Hellman. Ce protocole est baptisé le protocole DHWM (Diffie-Hellmann for Watermarking) : grâce aux propriétés du protocole de Diffie-Hellmann, il n'est pas nécessaire d'établir une ligne sécurisée, et le nombre de transferts d'images est réduit. C'est D. Augot qui était responsable de cette action. La réalisation est due à D. Augot et C. Fontaine. Ces travaux ont fait l'objet d'une présentation à ESORICS'98 [32], et d'un article *invité* à un numéro spécial IEEE [14] sur les techniques de marquage d'images. C. Fontaine est l'auteur d'un article au journal *Pour la Science* et d'une conférence à EUROFORUM [62, 46].

Les travaux du projet se poursuivent dans ce domaine, en collaboration avec C. Fontaine (LIFL), le projet FRACTALES, Telecom-Paris et le LIX. Le responsable du groupe de travail est M. Brunet[9], ingénieur du corps des télécommunications, qui vient d'être affecté pour trois ans à L'INRIA.

5 Contrats industriels (nationaux, européens et internationaux)

Notre collaboration avec la société COGENIT ainsi que l'étude qui s'intitule, *Analyse de trains binaires*, en partenariat avec Thomson-CSF et la DGA, se sont poursuivies cette année.

matics) consortium européen, managé par ERCIM, qui regroupait des partenaires culturels, tels les ministères de la culture en France ou en Grèce ou bien l'agence photographique F. Alinari en Italie, ou encore la *Royal commission for Historical Monuments* en Angleterre ; des sociétés d'informatique, tels BULL, FINSIEL (Italie) ou SSL (UK) ; des organismes de recherche, tels l'INRIA ou le CNR-CNUCE en Italie.

9. www-rocq.inria.fr/codes/watermarking

Une étude pour le CCETT de Rennes portant sur les codes CORTEX (voir §4.3) est en train de se finaliser.

Collaboration COGENIT-CODES : Réalisation d'un PCBL, 1997–99.
La société COGENIT a répondu en 1996 à un appel d'offre de l'ANVAR, en proposant la réalisation d'un "*Paquetage Cryptographique de Base Logiciel*" (PCBL). Le dossier, qui prévoit la participation de l'INRIA comme expert, a été accepté fin 1996. Dans le cadre de ce travail, une convention COGENIT – INRIA a été signée début 1997. Cette convention prévoyait une collaboration de deux ans pour la réalisation d'un produit cryptographique. Ce produit contient les fonctionnalités de signature numérique et de chiffrement et doit s'intégrer dans des machines Unix (ou Linux) fonctionnant sur le réseau Internet.

Le but est de mettre ce logiciel en accès libre et gratuit sur un serveur "ftp anonyme" de l'INRIA. La société COGENIT ne tirera de profit que des travaux d'ingénierie éventuels dérivés de ce produit, le logiciel servira en quelque sorte de "support publicitaire" et de démonstration de compétence. Le responsable de cette action, pour CODES, est N. Sendrier.

Dans ce travail, le projet CODES était maître d'œuvre et impliqué dans tout ce concerne les choix de primitives cryptographique et dans les protocoles. Intervient également le projet ALGO pour la résolution de certains problèmes algorithmiques, notamment la génération de grands nombres premiers pour les cryptosystèmes à clé publique. Enfin l'action IPV6 devra aider à l'intégration du logiciel dans le monde Unix et Internet, en particulier en prenant en compte les standards existants et à venir.

Un algorithme de signature digitale (Scrhypp) a été développé et l'on a obtenu en juin 1998 une autorisation de fourniture du SCSSI (Service Central de la Sécurité des Systèmes d'Information). C. Pourcelot a effectué un stage d'ingénieur de 12 mois financé par une bourse FONGECIF, d'Octobre 98 à Octobre 99. Elle a poursuivi le déploiement du logiciel Scrhypp pour des agents de courrier électronique ainsi que l'étude des évolutions du logiciel, en particulier pour des possibilités de chiffrement [71]. D'autre part, H. Alavoine a effectué un stage de fin d'étude (IUT de Villetaneuse) sur les générateurs aléatoires intervenant dans Scrhypp [58]. Ces deux stagiaires ont été dirigés par N. Sendrier.

6 Actions régionales, nationales et internationales

6.1 Actions nationales

Collaboration scientifique et échanges se sont poursuivis en 1999, avec les organismes d'enseignement et/ou de recherche. Les lieux de rencontre sont les groupes de recherche de type CNRS, les différents séminaires et l'activité au sein des écoles doctorales.

Le projet entretient des liens privilégiés avec les Universités de Caen, Limoges, Paris 6 et Toulon grâce à l'action des chercheurs extérieurs du projet issus de ces universités. Les chercheurs extérieurs interviennent dans diverses écoles doctorales et animent des séminaires. Ils soutiennent notre politique d'ouverture vers les universités.

Notre collaboration scientifique, avec nos chercheurs extérieurs, a aussi pour objectif d'accroître notre domaine de compétences en mathématiques. Nous avons besoin de spécialistes en théorie de groupes finis (T. Berger), en théorie algébrique des nombres (F. Laubie) et en

géométrie algébrique (D. Le Brigand). Ceci se concrétise par des travaux en commun ou des co-directions de thèses.

6.1.1 Contrats nationaux

Dans le contexte national, un contrat a été établi en 98 entre l'INRIA et les Écoles de Coëtquidan pour une durée de trois ans. Les partenaires sont respectivement le projet Codes et le Centre de Recherche des Écoles de Coëtquidan (CREC), nouvellement créé. P. Charpin est chargée de superviser les activités scientifiques de l'équipe *Mathématiques appliquées à la sécurité des systèmes d'information* et d'établir un ensemble d'interactions entre ce groupe et Codes. Des stagiaires sont accueillis chaque année; É. Filiol et D. Vianne, enseignants aux Écoles de Coëtquidan sont aussi chercheurs doctorants au projet. C'est dans le cadre de ce partenariat que nous avons organisé le colloque international *Workshop on Coding and Cryptography* en janvier 99.

6.1.2 Groupes de recherche

Le projet participe à deux groupements de recherche nationaux :

- GDR *Algorithmique, Modèles, Infographie* (AMI), équipe *Protection des Communications*, responsable D. Le Brigand.

- GDR MEDICIS, équipe *Codage*, responsable D. Augot.

Dans le cadre du GDR AMI, P. Charpin et B. Vallée (professeur à l'université de Caen), ont la responsabilité du groupe de travail intitulé *Codage et Cryptographie.*

L'intérêt de ces groupes de travail, qui ont fait l'objet d'un appel d'offre, est de regrouper la communauté nationale des chercheurs relevant d'un même thème scientifique. La dernière réunion a pris la forme, cette année, d'une école de printemps organisée par l'Inria à Batz-sur-mer en Juin 99[10].

Le projet entretient des relations suivies avec la DGA. Tous les membres du projet CODES participent activement au séminaire *Cryptographie, Codes et Algorithmique* qui a lieu une fois par mois à la DGA. Le but de ces réunions est d'entretenir des échanges scientifiques entre les chercheurs et les ingénieurs, et aussi entre les représentants des secteurs publics et industriels. Le séminaire est organisé par P. Loidreau[11] depuis Octobre 99.

D. Augot est chargé de l'organisation du séminaire du projet CODES.

A. Canteaut participe au groupe de travail *Signature Electronique* organisé par le club CSA (Cards, Systems and Applications) pour la rédaction d'un livre blanc sur la signature électronique. Le Club CSA regroupe des industriels, les fournisseurs de services et différents organismes impliqués dans les systèmes à base de carte à puce.

10. www-rocq.inria.fr/codes/Anne.Canteaut/Ecole/index.html
11. www-rocq.inria.fr/codes/Pierre.Loidreau/CCA/cca.html

6.1.3 Participations à des instances nationales

Plusieurs membres du projet participent à des commissions de spécialistes :

- Université de Caen, 27ème section (cnu) : C. Carlet.
- Université de Limoges, 25ème section (cnu) : T. Berger, P. Charpin, F. Laubie, D. Le Brigand.
- Université du Var, 27ème section (cnu) : C. Carlet, P. Charpin, S. Harari.
- Université de Marseille-Luminy, 27ème section (cnu) : S. Harari.
- Université Paris 6, 25ème section (cnu) : D. Le Brigand.

T. Berger est responsable de l'école doctorale de Mathématiques de l'université de Limoges.

P. Charpin est membre du comité d'administration de la Société des Personnels Enseignants et Chercheurs en Informatique en France (SPECIF).

L. Pecquet représente les doctorants au comité de l'UR de Rocquencourt.

6.2 Actions internationales

6.2.1 Organisation de rencontres, expertises

Le projet participe régulièrement à l'expertise des travaux de recherche pour les revues ou conférences internationales. On peut citer notamment pour cette année, les revues *IEEE on Information Theory*, *IEEE on Communications*, *Design, Codes and Cryptography*, *Journal of Theoretical Computer Sciences*, *Finite Fields*, le colloque *IEEE symposium on Information Theory* (ISIT).

Organisation de rencontres internationales :

- C. Carlet est membre de comité de programme de *International Conference on Sequences and Their Applications* (SETA), Singapour, décembre 1999.
- P. Charpin est membre du comité de programme de *13th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (AAECC13), Hawai, USA, Novembre 1999.
- P. Charpin est membre du comité de programme de *IEEE Symposium on Information Theory* (ISIT2000), qui aura lieu a Sorrente, Italie, en Juin 2000.
- F. Laubie a organisé un colloque international en théorie algébrique des nombres à Limoges les 17 et 18 novembre 1999.
- Les membres du projet ont organisé le colloque international *Workshop on Coding and Cryptography*, qui a eu lieu en Janvier 1999 à Paris [12].

12. www-rocq.inria.fr/codes/WCC99

- **Spécial issue in Coding and Cryptography**, Responsable : Claude Carlet, à paraître dans la revue Discrete Applied Mathematics, Editeurs associés: P. Charpin (INRIA-Rocquencourt), M. Girault (SEPT,Caen), G. Kabatiansky (IPPI, Moscou), H. VanTilborg (Eindhoven).

D. Augot est beta-testeur pour ALDOR, continuateur du compilateur Axiom de NAG.

6.2.2 Accueils de chercheurs étrangers

Le projet a une politique d'invitation "large", au plan national et au plan international. Cette année, S. Litsyn (Université de Tel-aviv, Israël) a séjourné 4 mois au projet. D'autre part, John T. Coffey (Université de Michigan, USA) a effectué un séjour sabbatique de 6 mois. Le projet a accueilli, pour de courtes durées, en 1999 :

- David Haccoun (École Polytechnique de Montréal, Québec, Canada),
- Gaétan Haché (Université McGill, Montréal, Québec, Canada),
- Dmitrii Nogin (IPPI, Moscou, Russie),
- Pawel Wocjan (Université de Karlsruhe, IAKS, Allemagne),
- Victor Zyablov (Académie des Sciences de Moscou, Russie),
- Preda Mihailescu (ETH Zentrum, Zürich, Suisse).

7 Diffusion de résultats

7.1 Enseignement

Pour les écoles doctorales, notre activité est d'abord une collaboration concrète avec nos chercheurs extérieurs sur le contenu des cours, les sujets de recherche et l'encadrement des thésards et stagiaires. Outre les DEA de Caen, Limoges et Toulon, nous sommes particulièrement impliqués dans deux DEA parisiens :

- *Méthodes algébriques*, Paris 6.
- *Algorithmique*, X-Ulm et universités Paris-centre, filière *Complexité, codage et Cryptographie.*

Les étudiants en thèse assurent des cours ou travaux dirigés, dans des universités à titre de moniteur, ou dans des écoles d'ingénieur. Précisément, les enseignements ou cours de formation permanente cette année ont été:

- "Codes Correcteurs", P. Charpin, DEA Algorithmique.
- C. Fontaine était ATER à l'Université d'Orsay.
- Cours de langage C, N. Sendrier, DEA, Limoges.

– TP d'informatique, L. Pecquet, Université de Paris 7 et École Polytechnique.

– N. Sendrier est chargé de TP à l'École Polytechnique, (tronc commun Informatique) depuis Octobre 99.

D. Augot a présenté un cours de cryptologie à l'OSSIR (Observatoire de la Sécurité d'Informations et des Réseaux, http://www.ossir.org/). L'OSSIR est une association de responsables "sécurité" (informaticiens) d'entreprises de taille importante. Le titre de la conférence était : *Cryptosystèmes, algorithmes et longueur de clés.*

A. Canteaut a participé aux *Journées de la Culture Mathématique* organisées par l'Académie de Versailles à destination des professeurs de mathématiques de l'enseignement secondaire. Le titre de sa conférence est "Mathématiques discrètes et cryptographie" (janvier 1999, Cergy-Pontoise).

7.2 Jurys de thèse

Les membres du projet ont participé aux jurys de thèse et habilitations suivants :

Décembre 98 E. Touratier,
Étude du typage dans le système de calcul scientifique Aldor
Thèse d'Université de Limoges.
Jury : T. Berger.

Décembre 98 A. Necer,
Suites récurrentes linéaires et séries formelles en plusieurs variables
Thèse d'Université de Limoges.
Jury : T. Berger (président).

Janvier 99 P. Langevin,
Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes
Habilitation à Diriger des Recherches de l'Université de Toulon.
Jury : C. Carlet, P. Charpin.

Mai 99 P. Guillot,
Fonctions courbes binaires et transformation de Möbius
Thèse de l'Université de Caen.
Jury : C. Carlet (direction), P. Charpin.

Juin 99 M. Girault,
Logarithme discret composite, hachage et redondance
Habilitation à Diriger des Recherches de l'Université de Caen.
Jury : C. Carlet.

Octobre 99 G. Skersys,
Calcul du groupe d'automorphismes des codes, Détermination de l'équivalence des codes,
Thèse d'Université de Limoges.
Jury : T. Berger (direction), P. Charpin (rapporteur), F. Laubie, N. Sendrier (co-direction).

Octobre 99 J.-F. MISARSKY,
Cryptanalyse et spécification de schémas de signature RSA avec redondance,
Thèse d'Université de Caen.
Jury : T. Berger (rapporteur).

7.3 Participation à des colloques

Les résultats obtenus par les participants du projet sont largement diffusés, dans des séminaires nationaux, à l'étranger lors de séjours ou dans les colloques internationaux.

Séjours courts dans des universités et laboratoires en 1999 :

- L. Pecquet : Université Technique du Danemark (Invité par T. Hoholdt), mars.
- L. Pecquet : Université de Sidney, Australie (Invité par J. Canon), pour 1 mois, à compter du 18 octobre.
- P. Charpin : Texas A&M University, College Station, USA (Invitée par B. Blackley), fin mars, début avril.

Participations aux colloques fin 98 et en 1999 :

- *SETA'98* - River View, Singapour,
  14-17 décembre 1998.
  Participant : C. Carlet.
- *WCC'99 - Workshop on Coding and Cryptography*, Paris, France,
  11-14 janvier 1999.
  Conférenciers : G. Skersys, A. Valembois.
  Participants : D. Augot, T. Berger, A. Canteaut, C. Carlet (Président du Comité de Programme), P. Charpin, É. Filiol, C. Fontaine, S. Harari, D. Le Brigand, P. Loidreau, L. Pecquet, N. Sendrier (Président du Comité d'Organisation).
- *Journée Arithmétique et Théorie de l'Information*, Marseille, France, 11 mars 1999.
  Conférencier : P. Loidreau.
- *FSE - Fast Software Encryption*, Rome, Italie, 24-26 mars 1999.
  Conférencière : A. Canteaut.
- *Eurocrypt'99*, Prague, République Tchèque, 2-6 mai 1999.
  Participants : É. Filiol, P. Loidreau.
- *27ième École de Printemps d'Informatique Théorique*, Batz-sur-Mer, France,
  31 mai au 4 juin 1999.
  Comité de programme : C. Carlet, P. Charpin, A. Canteaut
  Conférenciers : D. Augot, A. Canteaut, N. Sendrier.
  Participants : T. Berger, M. Brunet, É. Filiol, S. Harari, P. Loidreau, L. Pecquet, G. Skersys, A. Valembois.

- FQ5 - *Fifth International Conference on Finite Fields and Applications*, Portland, USA, 2-6 août 1999.
  Conférenciers : C. Carlet P. Loidreau, L. Pecquet.
- *Colloque Jeunes Chercheurs en Théorie des Nombres*, Lyon, France, 8-9-10 septembre 1999.
  Participant : L. Pecquet.
- *Journée Quantique*, Nice, France, 18 septembre 1999.
  Participants : P. Charpin, S. Litsyn (conférencier).
- *DIMACS Workhop on Codes and Association Schemes*, Newark, USA, 9-12 novembre 1999.
  Conférenciers : C. Carlet, N. Sendrier.
- *AAECC13*, Hawaii, USA, 14-19 novembre 1999.
  Conférencier : C. Carlet.
- *Seventh IMA International Conference on Cryptography and Coding*, Cirencester, UK, 20-22 décembre 1999.
  Conférencier : É. Filiol.

8 Bibliographie

Ouvrages et articles de référence de l'équipe

[1] D. Augot, « Description of minimum weight codewords of cyclic codes by algebraic systems », *Finite Fields and their Applications*, 2, 1996, p. 138–152.

[2] T. Berger, P. Charpin, « The permutation group of affine-invariant extended cyclic codes », *IEEE Transaction on Information Theory 42*, 6, novembre 1996, p. 2194–2209.

[3] A. Canteaut, F. Chabaud, « A new algorithm for finding minimum-weight words in a linear code: application to primitive narrow-sense BCH codes of length 511 », *IEEE Transactions on Information Theory 44*, 1, janvier 1998, p. 367–378.

[4] C. Carlet, P. Guillot, «A characterization of binary bent functions», *Journal of Combinatorial Theory, Series A 76*, 2, 1996, p. 328–335.

[5] P. Charpin, *Open problems on cyclic codes*, *I*, Handbook of Coding Theory, V.S.Pless and C.W. Huffman (eds) and, R.A. Brualdi (assistant editor), 1998.

[6] É. Filiol, C. Fontaine, «Highly nonlinear balanced Boolean functions with a good correlation-immunity», *in: Advances in Cryptology - EUROCRYPT'98*, *Lecture Notes in Computer Science*, 1403, Springer Verlag, p. 475–488, 1998.

[7] G. Haché, D. Le Brigand, «Effective construction of algebraic geometry codes», *IEEE Transaction on Information Theory 41*, Numéro spécial : Algebraic Geometry Codes, 6, 1996, p. 1615–1628.

[8] N. Sendrier, «On the dimension of the hull», *SIAM Journal on Applied Mathematics 10*, 2, mai 1997, p. 282–293.

Livres et monographies

[9] D. Augot, C. Carlet (éditeurs), *Livre des Résumés, International Workshop on Coding and Cryptography - (WCC'99), Paris, France, 11-14 janvier*, Publication INRIA, 1999.

[10] L. Pecquet, *A first course in family MAGMA, the computer algebra system*, Springer-Verlag, 1999, à paraître.

Thèses et habilitations à diriger des recherches

[11] C. Fontaine, *Contribution à la recherche de fonctions booléennes hautement non linéaires, et au marquage d'images en vue de la protection des droits d'auteur*, thèse de doctorat, Université Paris 6, novembre 1998.

[12] G. Skersys, *Calcul du groupe d'automorphismes des codes, détermination de l'équivalence des codes*, thèse de doctorat, Université de Limoges, octobre 1999.

Articles et chapitres de livre

[13] Y. Aubry, D. L. Brigand, « Imaginary bicyclic biquadratic function fields in characteristic two», *Journal of Number Theory*, 77, 1999, p. 36–50.

[14] D. Augot, J.-M. Boucqueau, J.-F. Delaigle, C. Fontaine, E. Goray, «Secure delivery of images over open networks», *Proceedings of the IEEE 87*, 7, juillet 1999, p. 1251–1266, (Special Issue on "Identification and protection of multimedia information"), article invité.

[15] T. Berger, P. Charpin, «The automorphism group of BCH codes and of some affine-invariant codes on an extension field», *Designs Codes and Cryptography 18*, 1/3, 1999, p. 29–53.

[16] T. Berger, «New classes of cyclic extended Goppa codes», *IEEE Transactions on Information Theory 45*, 4, 1999, p. 1264–1266.

[17] T. Berger, « On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes», *Finite Fields and their Applications*, 1999, à paraître.

[18] F. Blanchet, G. Bommier, «Binary quasi-cyclic Goppa codes», *Designs Codes and Cryptography*, 1999, à paraître.

[19] P. Camion, A. Canteaut, « Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography», *Designs, Codes and Cryptography*, 16, 1999, p. 121–149.

[20] A. Canteaut, P. Charpin, H. Dobbertin, « Binary m-sequences with three-valued cross-correlation: A proof of Welch conjecture», *IEEE Transactions on Information Theory*, 1999, à paraître.

[21] A. Canteaut, P. Charpin, H. Dobbertin, «Couples de suites binaires de longueur maximale ayant une corrélation croisée à trois valeurs : conjecture de Welch», *Comptes Rendus de l'Académie des Sciences t.328*, Serie 1, 1999, p. 173–178.

[22] A. Canteaut, P. Charpin, H. Dobbertin, «Weight divisibility of cyclic codes, highly non-linear functions on GF(2^m) and crosscorrelation of maximum-length sequences», *SIAM Journal on Discrete Mathematics*, 1999, à paraître.

[23] C. Carlet, P. Charpin, V. Zinoviev, « Codes, bent functions and permutations suitable for DES-like cryptosystems », *Designs Codes and Cryptography*, 15, 1998, p. 125–156.

[24] C. Carlet, « Z_{2^k}-linear codes », *IEEE Transactions on Information Theory 44*, 4, 1998, p. 1543–1547.

[25] C. Carlet, « On cryptographic propagation criteria for Boolean functions », *Information and Computation*, 151 (Special Issue on Cryptology in Honor of Professor Arto Salomaa on Occasion of His 65th Birthday) article invité, 1999, p. 32–56.

[26] P. Charpin, A. Tietavainen, V. Zinoviev, « On the Minimum Distances of Non-binary Cyclic Codes », *Designs Codes and Cryptography 17*, 1/3, 1999, p. 81–85.

[27] C. Fontaine, « On some cosets of the first-order Reed-Muller code with high minimum weight », *IEEE Transactions on Information Theory 45*, 4, mai 1999, p. 1237–1243.

[28] F. Laubie, M. Saîne, «Ramification of some automorphisms of local fields», *Journal of Number Theory*, 1999, à paraître.

[29] F. Laubie, « A recursive definition of p-ary addition without carry », *Journal de théorie des nombres de Bordeaux*, 1999, à paraître.

[30] N. Sendrier, «Finding the permutation between equivalent linear codes: the support splitting algorithm», *IEEE Transactions on Information Theory*, 1999, à paraître.

[31] N. Sendrier, « On the concatenated structure of a linear code », *Journal of AAECC*, 1999, à paraître.

Communications à des congrès, colloques, etc.

[32] D. Augot, C. Fontaine, J.-F. Delaigle, « DHWM: a scheme for managing watermarking keys in the Aquarelle multimedia distributed system », *in : Computer Security - ESORICS 98*, *Lecture Notes in Computer Science*, 1485, Springer Verlag, p. 241–255, 1998.

[33] D. Augot, «Introduction à la cryptologie des courbes elliptiques», *in : 27e École de printemps d'informatique théorique, Codage et cryptographie*, Batz-sur-Mer, France, juin 1999.

[34] T. Berger, « Cyclic alternant codes induced by an automorphism of a GRS code », *in : Finite fields: Theory, Applications and Algorithms, (août 97)*, R. Mullin, G. Mullen (éditeurs), *225*, AMS, Contemporary Mathematics, p. 143–154, Waterloo, Canada, 1999.

[35] A. Canteaut, P. Charpin, H. Dobbertin, «A new characterization of almost bent functions», *in : Fast Software Encryption 99*, L. Knudsen (éditeur), *Lecture Notes in Computer Science*, 1636, Springer-Verlag, p. 186–200, 1999.

[36] A. Canteaut, N. Sendrier, « Cryptanalysis of the original McEliece cryptosystem », *in : Advances in Cryptology - ASIACRYPT'98*, *LNCS*, 1514, Springer-Verlag, p. 187–199, 1998.

[37] A. Canteaut, «Fonctions booléennes et cryptographie», *in : 27e École de printemps d'informatique théorique, Codage et cryptographie*, Batz-sur-Mer, France, juin 1999.

[38] C. Carlet, S. Dubuc, « On generalized bent and q -ary perfect nonlinear function», *in : Fifth International Conference on Finite Fields and Applications*, Augsburg, Allemagne, août 1999.

[39] C. CARLET, P. GUILLOT, «A representation of Boolean functions», *in : AAECC'13, Novembre 99*, *LNCS*, Springer Verlag, 1999. À paraître.

[40] C. CARLET, «Recents results on bent functions», *in : Proceedings on International Conference on Combinatorics, Information Theory and Statistics, ICC'97 (Juillet 97)*, Portland, USA, 1998. À paraître.

[41] C. CARLET, «On Kerdock codes», *in : Finite Fields and their Applications, (août 97)*, R. Mullin, G. Mullen (éditeurs), *Contemporary Mathematics*, 225, American Mathematical Society, p. 155–163, Waterloo, Canada, 1999.

[42] C. CARLET, « One-weight $\mathbf{Z}_4$-linear codes », *in : International conference on Coding Theory, Cryptography and Related Areas, Avril 1998*, *Lecture Notes in Computer Science*, Springer Verlag, 1999. À paraître.

[43] C. CARLET, « Recent developments in the research on bent and perfect nonlinear functions », *in : DIMACS Workshop on Codes and Association Schemes*, Rutgers University, Piscataway, NJ, USA, Novembre 1999.

[44] É. FILIOL, «Designs, intersecting families and weight of boolean functions», *in : 7th IMA Conference on Cryptography and Coding, Décembre 99*, *Lecture Notes in Computer Science*, Springer Verlag, 1999. À paraître.

[45] C. FONTAINE, «Highly nonlinear boolean functions», *in : Journées Complexité, Modèles Finis et Bases de données, GDR ALP*, Université Paris 7, février 1999.

[46] C. FONTAINE, «Watermarking», *in : Sécurité des échanges sur Internet, EUROFORUM*, Paris, novembre 1999.

[47] S. LITSYN, «Quantum codes and quantum error-detection», *in : Workshop on Quantum Computing*, Nice, France, septembre 1999.

[48] P. LOIDREAU, «Codes dérivés de certains codes de Goppa», *in : Journée ATI*, Marseille, France, mars 1999.

[49] P. LOIDREAU, «On the factorization of trinomials over GF(3)», *in : Fifth International Conference on Finite Fields and Applications*, Augsburg, Allemagne, août 1999.

[50] L. PECQUET, « An algorithm to get some factors of bivariate polynomials without factoring», *in : Fifth International Conference on Finite Fields and Applications*, Augsburg, Allemagne, août 1999.

[51] N. SENDRIER, G. SKERSYS, «Permutation groups of error-correcting codes», *in : Workshop on Coding and Cryptography - (WCC'99), 10-14 janvier*, Paris, France, janvier 1999.

[52] N. SENDRIER, «Introduction à la théorie de l'information», *in : 27e École de printemps d'informatique théorique, Codage et cryptographie*, Batz-sur-Mer, France, juin 1999.

[53] N. SENDRIER, « Structural attacks on code-based cryptosystems and related problems », *in : DIMACS Workshop on Codes and Association Schemes*, Rutgers University, Piscataway, NJ, USA, Novembre 1999.

[54] A. VALEMBOIS, «Recognition of a binary linear code as a vector subspace», *in : Winter Scool on Coding and Information Theory 1998*, décembre 1998.

[55] A. VALEMBOIS, «Detection and recognition of a binary linear code», *in : WCC'99*, janvier 1999.

Rapports de recherche et publications internes

[56] D. Nogin, «Generalized Hamming weight as weight function», *rapport de recherche n° RR-3762*, INRIA, septembre 1999, `http://www.inria.fr/RRRT/RR-3762.html`.

[57] N. Sendrier, « The support Splitting Algorithm », *rapport de recherche n° RR-3637*, INRIA, mars 1999, `http://www.inria.fr/RRRT/RR-3637.html`.

Divers

[58] H. Alavoine, « Création et intégration d'un générateur pseudo-aléatoire cryptographique », Mémoire de stage de fin d'Études, IUT Villetaneuse, 1999.

[59] D. Augot, L. Pecquet, « A lifting method to replace factorization in Sudan's algorithm », 1999, soumis pour publication.

[60] T. Berger, «Goppa and related codes invariant under a prescribed permutation», 1999, soumis pour publication.

[61] S. Cutajar, C. Libert, « Simulation d'une chaîne de transmission numérique », Mémoire de stage de fin d'Études, École Spéciale Militaire de Saint-Cyr/Écoles de Coëtquidan, 1999.

[62] C. Fontaine, « Tatouage des images numériques et protection des droits d'auteur », 1999, à paraître.

[63] S. Harari, «HCC : une fonction de hachage utilisant les codes et corrélations», 1998, soumis pour publication.

[64] F. Laubie, «Linear ternary Greedy codes», 1997, soumis pour publication.

[65] F. Laubie, «Ramification des polynômes de Chebyshev», 1997, soumis pour publication.

[66] F. Laubie, «Ramification de certaines extensions de Lie», 1998, soumis pour publication.

[67] P. Loidreau, N. Sendrier, « Weak key in McEliece public-key cryptosystem », 1999, soumis pour publication.

[68] P. Loidreau, «Codes derived from binary Goppa codes», 1999, soumis pour publication.

[69] G. Olocco, «Décodage itératif des codes Cortex», Mémoire de stage de DEA, Université de Paris 7, 1999.

[70] A. Otmani, «Recherche de codes auto-duaux sous forme de codes Cortex», Mémoire de stage de DEA, Université de Limoges, 1999.

[71] C. Pourcelot, «Portage d'un logiciel cryptographique de Linux vers Windows NT», Mémoire de stage de fin d'Études, C.N.A.M., 1999.

[72] N. Sendrier, G. Skersys, « On computing the permutation groups of error-correcting codes», 1998, soumis pour publication.

[73] M. Trabbia, «Attaques par corrélation rapides de générateurs pseudo-aléatoires pour la cryptographie», Rapport de stage d'Option de l'École Polytechnique, 1999.

[74] A. Valembois, « Detection and recognition of a binary linear code», 1999, soumis pour publication.