Projet CODES

Codes et Protection de l'Information

Localisation : *Rocquencourt*

Mots-clés : code correcteur, erreur, transmission de signal, algorithme, protection de l'information.

1 Composition de l'équipe

Responsable scientifique

Paul Camion, directeur de recherche CNRS

Responsable permanent

Pascale Charpin, directeur de recherche INRIA

Secrétaire

Christelle Guiziou-Cloitre

Conseiller scientifique

Guy Chassé, Ecole des Mines de Nantes

Personnel Inria

Nicolas Sendrier, Chargé de Recherche
Daniel Augot, Chargé de Recherche

Chercheurs doctorants

Francis Blanchet, Education Nationale
Gaétan Haché, Boursier INRIA, depuis Janvier 93
Anne Canteaut, Boursière DRET, depuis Septembre 93
Grégoire Bommier, Contractuel Ministère Défense, depuis Septembre 95
Caroline Fontaine, Boursière MENESR, depuis Septembre 95

Chercheurs extérieurs

Thierry Berger, Université Limoges
Claude Carlet, Université Caen
François Laubie, Université Limoges
Sami Harari, Université Toulon
Dominique Le Brigand, Université Paris 6
Jacques Wolfmann, Université Toulon

Chercheurs Invités

Edward F. Assmus, Jr., Université de Lehigh, USA, du 9 mai au 8 juillet 96
Simon Litsyn, Université de Tel Aviv, Israel, du 1er août au 30 septembre 96
Thomas Ericson, Université de Linköping, Suède, du 2 octobre au 30 octobre 96

2 Présentation du projet

Le domaine de recherche du projet *CODES* est centré sur l'étude la *Protection de l'Information* numérique. Comme il est expliqué dans ce rapport, qui décrit nos différentes activités et orientations, 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 et la construction effective 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 actuellement 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 (cf. Section 3.3 et 4.).

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. A titre d'exemple, ce profil est demandé actuellement pour concevoir et mettre en œuvre les algorithmes intervenant dans les carte à puces.

Axes de recherche

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. Surtout la *théorie algèbrique des codes* et la *cryptographie* ont des thèmes de recherche communs, thèmes "centraux", ainsi les fonctions booléennes pour le chiffrement ou l'étude des codes aléatoires. Le projet s'est investi dans ces deux voies de recherche, encore plus fortement cette année.

Les codes correcteurs servent à protéger une information transitant à travers un canal de transmission. Ce canal peut être une ligne téléphonique, une liaison radio ou encore un support magnétique ou optique : bande magnétique ou disque compact. Il sera généralement perturbé par un bruit dépendant de l'environnement et de la nature du canal. Le codage consiste en l'ajout d'une redondance pour combattre les effets du bruit. 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.

Les applications les plus familières des codes correcteurs sont l'utilisation des codes de Reed-Solomon dans le disque compact. Les plus importantes concernent les télécommunications, en particulier les liaisons avec les satellites et les sondes spatiales. Le disque compact est un exemple remarquable de ligne très bruitée où l'on peut corriger les erreurs dues aux empreintes digitales, poussières, salissures ou érosions laissant une trace d'environ 2,5 mm sur le disque qui, pour 74 minutes de musique, est le support d'environ 20 milliards de bits, élaborés sur la saisie de deux fois 16 bits d'information, 44,100 fois par seconde.

Depuis les premiers codes de HAMMING et surtout la découverte des fameux codes BCH (1960), la Théorie Algébrique des Codes Correcteurs connait un développement constant. On peut mesurer ceci à

la vivacité des sessions qui lui sont consacré dans le colloque International de Théorie de l'Information organisé par la société IEEE. La recherche *pure* sur les codes correcteurs consiste en l'étude in abstracto des meilleurs codes possibles. On est ainsi amené à construire des codes ayant une structure algébrique de plus en plus complexe, en utilisant tous les outils de Mathématique Discrète (algèbre des structures finies, combinatoire, géométries finies...). L'autre versant de la recherche se situe au niveau de la *performance des codes*, ce qui impose la recherche systématique de tous les paramètres d'un code donné; l'existence et la complexité d'algorithmes de décodage sont alors un élément de l'étude. Ainsi le domaine de recherche, bien que centré sur l'étude d'un objet "mathématique", doit intégrer les outils modernes de l'Informatique Théorique, notamment l'Algorithmique et le Calcul Formel.

Le dévelopement récent de la *cryptographie* montre que la recherche que nous venons de décrire s'applique généralement en codage. En effet, les liens existant entre la cryptographie et la théorie des codes correcteurs se concrétisent en de nouveaux thèmes de recherche. Il peut s'agir par exemple de construire des protocoles dont la confidentialité est basée sur un problème NP-complet relevant de la théorie des codes. Plus généralement, l'utilisation des fonctions booléennes, de la théorie des corps finis ou de certains algorithmes de codage, nécessite la compétence de spécialistes de théorie des codes.

La cryptographie a pour but de préserver l'intégrité de l'information numérique. Les lignes de transmission et les enregistrements numériques sont exposés à la lecture et éventuellement à l'effacement et à la réécriture. La provenance d'un message est à priori incertaine.

Des solutions à ces problèmes sont proposées mais la difficulté d'obtention d'une sécurité démontrable rend la tâche immense. *Tous les crypto-algorithmes conventionnels sans exception ont été conçus sans preuve formelle de leur sécurité.* A titre d'exemple, Eli Biham a montré tout-à-fait récemment que le DES utilisé en triple passes, qui a la faveur aujourd'hui, et quels que soient les modes pour chaque passe, a une sécurité très inférieure à ce que pourrait faire espérer les $168 = 3 \times 56$ bits de clé.

De plus, les débits demandés aujourd'hui requièrent la recherche de nouveaux algorithmes. Dans ce contexte, le projet obtient des résultats qui permettent de répondre aux besoins en chiffrement à grand débit demandés dans diverses applications (voir §3.3.3, troisième paragraphe).

Le chiffrement, qui assure la confidentialité, par exemple dans les transmissions radio, est l'une des multiples applications de la cryptographie. Mais les applications les plus importantes concernent l'authentification des correspondants, la garantie d'intégrité du message et la signature des textes numériques qui doit rendre impossible la répudiation d'un ordre. Le travail effectué pour Aquarelle (voir §4) peut être placé dans ce contexte.

Généralement parlant, l'ensemble des actions de recherche que nous avons décrites fournissent les matériels scientifiques indispensables à la conception de toute application, dans les domaines concernés.

3 Actions de recherche

3.1 Paramètres des codes correcteurs

3.1.1 Etude de systèmes d'equations sur les corps finis

Participants : Daniel Augot, Françoise Levy-dit-Vehel

Ces dernières années, l'évolution des logiciels de calcul formel et le développement du thème *Géométrie algèbrique 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 du poids minimum (capacité de correction) de certains codes, ou pour l'étude du rayon de recouvrement, paramètre qui mesure la distance d'un mot quelconque au code utilisé. Des techniques de décodage, fonées sur la recherche de bases standards, sont aussi à l'étude dont les applications intéressent le codage en général.

Mots de poids minimum et décodage algébrique D. Augot a introduit, dans sa thèse, une méthode de recherches de mots de poids minimal dans un code linéaire, utilisant des techniques de bases de Groebner et les possibilités du logiciel AXIOM. D. Augot a généralisé ces méthodes à presque tous les codes. Les éléments de base de ce prolongement sont publiés dans [337]. Un autre article est en préparation. Toutefois, le problème de la recherche de mots de poids minimal est un problème NP-complet, et l'algorithme de Buchberger pour résoudre des systèmes d'équations algébriques montre vite ses limites. Il y a là une voie de recherche commune au calcul formel et au codage.

Le décodage des codes correcteurs connaît un regain d'intêret parmi les codeurs (voir les recherches menées pour la cryptographie §3.3.2). Il existe des codes performants que l'on ne sait pas décoder, ainsi les *codes résidus quadratiques* — qui sont des codes cycliques. D'autre part, une meilleure compréhension des méthodes de décodage et de la résolution des systèmes algébriques apparait dans la communauté. En effet, il est maintenant bien compris que décoder revient à calculer une base de Groebner d'un idéal, appelé idéal des localisateurs. Il est maintenant possible de décoder tout code cyclique, de petite longueur, jusqu'à la vraie distance minimale en calculant une base de Groebner. Daniel Augot a présenté à Linz (IMACS'96) ses travaux sur le sujet [357]. La complexité du décodage des codes cycliques, n'est pas, à l'instar des codes linéaires, prouvée NP-complète.

Rayon de recouvrement Pendant son post-doctorat à Tel-Aviv, F. Levy-dit-Vehel a étudié avec S. Litsyn le comportement asymptotique du rayon de recouvrement de codes classiques, tels les codes BCH et les codes de Goppa. Des améliorations importantes par rapport aux résultats connus ont été obtenues. Le problème étant exprimé en termes de résolution de systèmes d'équations non linéaires sur des corps finis, les auteurs utilisent des sommes exponentielles bien adaptées à la résolution de ce type de systèmes [354].

3.1.2 Equivalences de codes

Participants : Thierry Berger, Pascale Charpin, Nicolas Sendrier

Reconnaitre deux codes équivalents, reconnaitre 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.

Automorphismes des codes invariants sous le groupe affine. Il s'agit de codes cycliques étendus primitifs. Ils recouvrent des classes importantes telle celle des codes BCH.

T. Berger a poursuivi l'étude des groupes d'automorphismes des codes affines-invariants. Ses résultats, relevant de la théorie des groupes finis, apportent des éléments décisifs pour caractériser les groupes de permutations de n'importe quel code [340].

T. Berger a prolongé son étude avec P. Charpin. Utilisant les travaux de Delsarte (1969) et la description des codes affine-invariants par antichaîne, due à P. Charpin (1987), les auteurs 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 va paraitre, sous forme de *regular paper* dans IEEE Transaction on Info. Theory (voir [338, 339]). Un autre article est en préparation [358].

Dans [359], T. Berger montre comment le groupe d'automorphisme se déduit du groupe de permutations pour tous les codes affines-invariants. Il donne aussi les conditions d'équivalence de deux codes. T. Berger a passé son habilitation en Janvier 96 [332].

Codes équivalents. N. Sendrier a conçu et mis en œuvre un nouvel algorithme, permettant de tester l'équivalence de deux codes linéaires donnés. Cet algorithme utilise les invariants du *Hull* – i.e. intersection d'un code avec son dual – des codes linéaires et permet d'obtenir la permutation chaque fois que le groupe d'automorphisme du code est trivial et que son Hull est de petite taille. Il faut noter que ces propriétés sont généralement verifiées [380, 355]. Ce travail est à son début. Plusieurs études sont en cours, visant à déterminer les meilleures heuristiques et la complexité de cet algorithme. Les diverses applications possibles de l'algorithme, en relation avec la solidité de certains cryptosystèmes (voir §3.3.2), sont aussi à l'étude.

3.1.3 Codes et combinatoire

Participants : Pascale Charpin, Victor Zinoviev, Claude Carlet

Les chercheurs du projet s'intéressent aux propriétés générales sructurelles 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.

Suite à une étude sur la distribution de poids des translatés des codes BCH binaires 2-correcteurs, P. Charpin a mis en place des outils plus généraux [378]. Ce travail s'est poursuivi avec V. Zinoviev. Dans [347] les auteurs montrent notamment que les propriétés obtenues pour les BCH 2-correcteurs ne sont plus vraies pour des capacités de correction supérieures.

La dualité formelle de codes non linéaires est une propriété actuellement très étudiée. Des travaux récents sur les codes $\mathbf{Z}_4$ linéaires ont prouvé que dans certains cas, faire *passer* un code dans $\mathbf{Z}_4$ simplifie la structure du code. Par exemple, un code non-linéaire peut devenir linéaire. C. Carlet a approfondi une propriété de dualité récemment mise en évidence par A.R. Calderbank, N.J.A. Sloane et d'autres auteurs concernant les codes construits sur les anneaux de Galois. Parmi ces codes, on trouve les codes de Kerdock, et des analogues des codes de Preparata classiques. Ce travail a fait l'objet d'un article à *IEEE Transactions on Information Theory* [345].

3.1.4 Codes géométriques

Participants : Gaétan Haché, Dominique Le Brigand

Depuis les travaux de GOPPA (1960-70), on sait que les codes géométriques constituent une classe importante de codes correcteurs ; leurs "bons" paramètres et leur structure algébrique complexe les désignent naturellement pour certaines applications (construction de codes longs, protocole de protection...). Constructions et classifications sont en cours d'étude, qui nécessitent une collaboration étroite entre Mathématiciens, Théoriciens du Codage et spécialistes de Calcul Formel. L'apport des logiciels de Calcul Formel, qui dans ce contexte doivent être utilisés et même développés par des spécialistes, est très important.

Pour développer ce thème de recherche, le projet entretient des contacts étroits avec l'équipe de D. Lazard pour le calcul formel et avec D. Le Brigand, spécialiste de géométrie algébrique (université Paris 6).

D. Le Brigand a dirigé la thèse de G. Haché, boursier INRIA.

En théorie des nombres, de nombreux travaux portent sur le nombre de classes des corps quadratiques imaginaires. D. Le Brigand a étudié l'analogue de ce problème pour les corps de fonctions. Elle a donné toutes les extensions quadratiques imaginaires K de $k(x)$, où k est un corps fini, pour lesquelles le nombre de classes d'idéaux de la clôture intégrale de $k[x]$ dans K est égal à 2 (le cas 1 est connu). Ces résultats sont publiés dans les comptes-rendus du colloque AGCT4 (Arithmetic, Geometry and Coding Theory, Juin 93)[353].

D. Le Brigand a aussi classifié les corps de fonctions algébriques en une variable dont le nombre de points de la jacobienne est égal à deux. Ceci est publié dans la revue *Finite Fields and their Applications* [352].

G. Haché a soutenue, le 19 septembre 1996, sa thèse intitulée *Construction effective des codes géométriques*, Dans sa thèse, il traite des algorithmes de construction des codes géométriques, en deux parties complémentaires :

- présentation des notions mathématiques nécessaires à la compréhension des algorithmes,
- description détaillée de ces algorithmes et de leur implantation.

En particulier, on y trouve une description détaillée du logiciel qu'a réalisé G. Haché en AXIOM. Avec ce logiciel, qui implante entre autres l'algorithme de Brill-Noether, on peut faire tous les calculs nécessaires pour construire des codes géométriques définis à partir de courbes planes ; on peut entre autres effectuer la désingularisation des courbes planes, le calcul du genre, le calcul des bases des espaces vectoriels $L(D)$ associés à un diviseur D et le calcul de l'ordre (et l'évaluation le cas échéant) d'une fonction en toute place du corps des fonctions de la courbe. Bien que ce logiciel effectue des calculs très complexes, il est néanmoins efficace et convivial. Il se veut aussi un outil de recherche déjà apprécié par la communauté internationale du codage [349, 334, 372, 371].

Indépendamment de l'algorithme de Brill-Noether, G. Haché propose aussi dans sa thèse une construction effective propre à des codes géométriques particuliers obtenus par A. Garcia et H. Stichtenoth en 1995. Ces codes sont définis à partir d'extensions particulières de corps de fonctions du type d'Artin-Schreier avec lesquelles on peut construire, en théorie, une classe de codes dépassant la borne de Varshamov-Gilbert. Soulignons que la méthode de construction effective proposée par G. Haché, bien que toujours insuffisante en pratique, est la plus efficace connue à l'heure actuelle. Cette méthode a aussi permis à d'autres chercheurs de vérifier ou rejeter certaines hypothèses relatives à leurs recherches sur la construction explicite de tels codes.

3.1.5 Codes de Goppa

Participants : Francis Blanchet, Grégoire Bommier

Les codes de Goppa binaires sont souvent dits *quasi-aléatoires* — i.e. très "proches" des codes aléatoires. C'est sans doute pour cette raison qu'ils sont utilisés dans certains cryptosystèmes (voir §3.3.2). 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. Une partie de l'étude demandée par la DRET (voir §4) porte sur la structure des codes de Goppa binaires.

G. Bommier étudie dans le cadre de sa thèse les codes de Goppa binaires dont le groupe d'automorphisme est non trivial. En collaboration avec F. Blanchet, il a exhibé certaines contraintes explicites sur les paramètres, induisant la *quasi-cyclicité* d'un code de Goppa [360]. Une généralisation est en cours d'élaboration en vue de rendre les contraintes suffisantes.

3.2 Codes correcteurs : aspects algorithmiques

3.2.1 Calcul des poids des codes

Participants : Daniel Augot, Françoise Levy-dit-Vehel, Nicolas Sendrier

Un logiciel permettant le calcul de l'énumérateur des poids des codes binaires linéaires et de leurs translatés a été mis en œuvre par N. Sendrier en 1994. Celui-ci fait appel à des techniques algorithmiques pointues (code de Gray, polynômes de Krawtchouk pour la transformée de MacWilliams, ...), et s'est avéré performant puisqu'il a permis le calcul d'énumérateurs de poids encore inconnus. L'utilisation du logiciel a permis de démontrer l'équivalence de certains codes binaires [348]. Enfin le programme est utilisé de façon intensive pour diverses études ([347, 383, 377] et [370]).

F. Levy-dit-Vehel et D. Augot ont mené une étude sur *la distance duale des codes BCH*. Les résultats numériques prouvent notamment que la borne de Carlitz-Ushiyama peut être largement dépassée, dans

certains cas où l'on pensait qu'elle donnait une bonne approximation [336]. Ce travail a un intérét plus général, car plusieurs algorithmes, donnant une approximation de la distance minimal d'un code cyclique, ont été implémentés et optimisés. Ces logiciels sont maintenant disponibles pour d'autres tests.

3.2.2 Calcul dans les corps finis

Participants : Daniel Augot, Paul Camion

Une étude algorithmique a été menée par P. CAMION et D. AUGOT pour calculer le polynôme minimal d'un endomorphisme, ainsi que d'autres paramètres invariants (notamment les "diviseurs élémentaires"). Le problème de l'optimisation du calcul d'un vecteur cyclique a aussi été étudié. Le résultat principal est l'obtention d'un algorithme déterministe en $O(n^3)$ pour le calcul d'une base normale dans un corps fini. Les meilleurs algorithmes déterministes connus étaient de complexité $O(n^4)$. De plus, un algorithme de calcul du polynôme minimal de complexité $O(n^3)$ en moyenne sur un corps fini est proposé. La complexité dans le pire des cas est de $O(n^{3.5})$, alors qu'elle était $O(n^4)$ pour les algorithmes connus. Tous ces résultats constituent donc une avancée algorithmique en algèbre linéaire sur les corps finis.

Ces algorithmes ont été implantés en AXIOM, et, bien que déterministes, sont plus rapides que les algorithmes *probabilistes* déjà existant en AXIOM. Un article complet va paraître prochainement dans la revue *Linear Algebra and Its Applications.* [335]

3.3 Codage et cryptographie

3.3.1 Codage d'un corpus de mots

Participant : Nicolas Sendrier

N. Sendrier poursuit, en collaboration avec Ph. Guillot, une étude portant sur le codage des mots q-aires de poids et de longueur donnée. Différents aspects de ce problème ont été envisagés : solution exacte à faible coût algorithmique, et solution approchée en temps linéaire. Une partie des résultats a été présenté au workshop "Coding and Cryptography" [374].

3.3.2 Protocoles basés sur les codes correcteurs

Participants : Anne Canteaut, Nicolas Sendrier

A. Canteaut, en collaboration avec F. Chabaud (GRECC, ENS-Ulm), a élaboré un algorithme de recherche de mots de poids faible dans un code linéaire quelconque. Cet algorithme améliore notablement les performances de tous les algorithmes connus précédemment. [363, 341].

D'un point de vue cryptographique, il constitue une amélioration de toutes les attaques connues sur les systèmes cryptographiques fondés sur les codes correcteurs d'erreurs. Il existe en effet plusieurs systèmes de chiffrement à clef publique (systèmes de McEliece et de Niederreiter) et schémas d'identification (schémas de Girault, de Stern et de Véron) qui reposent sur la difficulté de trouver un mot de poids minimum dans un code linéaire dont seule une matrice génératrice est connue. Leur principal intérêt est qu'ils constituent désormais une des rares alternatives connues aux systèmes à clef publique fondés sur la théorie des nombres (RSA). Une étude très précise de la complexité de cette nouvelle attaque par la théorie des chaînes de Markov a montré que le système de chiffrement de McEliece employé avec ses paramètres originaux n'assure pas une sécurité satisfaisante [333].

Du reste, cet algorithme a également été utilisé dans l'optique de la théorie des codes puisqu'il a permis à Anne Canteaut de déterminer la distance minimale de certains codes BCH en longueur 511, qui était jusqu'à ce jour inconnue [364].

L'étude des *codes permutés* est un autre aspect de la recherche sur les protocoles 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. §3.1.2).

Une étude de la structure des *codes concaténés* du premier ordre à permis à N. Sendrier d'obtenir des résultats concernant l'utilisation de ces codes pour des systèmes cryptographiques à clé publique ; 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 [386]. Cette étude a des conséquences immédiates en cryptographie puisqu'elle montre que l'utilisation de ces codes dans des cryptosystèmes à clé publique de type McEliece ou Niedereitter, n'est pas fiable. Des travaux récents sur les cryptosystèmes à clé publique envisagent l'utilisation de codes concaténés dont le code externe est choisi dans une famille de codes géométriques et le code interne est un code de parité simple. Cette famille de codes concaténés permet d'éviter l'attaque mise au point par N. Sendrier en 1995. Il semble néanmoins possible de généraliser cette attaque et de fragiliser ainsi ce nouveau système.

3.3.3 Fonctions cryptographiques

Participants : Paul Camion, Anne Canteaut, Claude Carlet, Caroline Fontaine

Les fonctions booléennes sont un objet de codage, au sens large. Ainsi leur utilisation dans les protocoles de chiffrement ou dans la définition de séquences *fortement autocorrélées* est bien connue.

D'autre part, leurs propriétés ont surtout été étudiées par les théoriciens des codes. En effet, ces propriétés sont étroitement liées aux propriétés des codes cycliques. Plus précisemment, le degré d'une fonction détermine son appartenance à l'un ou l'autre des codes de Reed et Muller, codes de référence dans la théorie.

Il s'agit là d'un des thèmes de recherche important du projet. Le travail se poursuit surtout dans l'optique *cryptographique*. On veut étudier et construire des classes de fonctions qui augmentent la potentialité des systèmes ou leur résistance aux différentes cryptanalyses connues.

Les résultats sur les propriétés de non-linéarité et de non corrélation sont décrits ci-après. En outre, une étude est en cours sur les fonctions résistantes aux cryptanalyses linéaire et différentielle. Les participants à cette étude sont C. Carlet, P. Charpin et V. Zinoviev. Plusieurs articles sont en préparation. Dans ce contexte, apparaissent des codes cycliques binaires de grande dimension. Une étude complémentaire est menée avec A. Tietäväinen (cf. [369, 383]).

La haute non-linéarité Un 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. Une partie de l'étude demandée par la DRET (voir §4) se situe dans ce contexte.

C. Fontaine mène une étude exploratoire de la propriété de non linéarité, s'appuyant sur un corpus de fonctions ayant une représentation courte. Ce corpus, algébriquement très structuré, est aisément manipulable. Les premiers résultats montrent surtout une bonne distribution des éléments du corpus dans l'ensemble des fonctions booléennes. Ces résultats ont été présentés à PRAGOCRYPT'96 [370]. C. Fontaine a exposé ses résultats dans plusieurs séminaires, au SCSSI et à *l'Ecole d'hiver de Théorie du Codage* (Décembre 96, Suède).

Fonctions courbes Malgré un intense travail de recherche sur les fonctions courbes, deux classes générales, seulement, ont été déterminées jusqu'en 1993 où deux nouvelles classes ont été déterminées par C. Carlet.

C. Carlet a ensuite obtenu une définition unifiée des fonctions courbes connues. Son travail sur les fonctions courbes s'est poursuivi cette année. Il a proposé une caractérisation originale des fonctions courbes utilisant des outils de géométrie discrète [342, 343]. Il a également introduit une nouvelle construction secondaire de fonctions courbes qui généralise toutes celles qui étaient déjà connues et en a déduit d'autres classes [366]. Il a enfin caractérisé les fonctions dites *hypercourbes*, de restrictions courbes [367, 368]. Plusieurs publications sont en préparation.

Fonctions t-résilientes et applications cryptographiques 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 flux. Elle sont reliées aux codes du fait que les codes forment des tableau orthogonaux et que ces tableaux permettent de caractériser les fonctions résilientes. P. Camion et A. Canteaut ont généralisé les notions de fonctions sans-corrélation et de fonctions résilientes aux fonctions définies sur un alphabet fini quelconque et ont donné de nouvelles caractérisations de ces propriétés (EUROCRYPT"96,[361]). Ceci a conduit à une construction générale par composition qui produit de nouvelles fonctions résilientes ayant un grand nombre de variables. L'utilisation de ces fonctions débouche sur la construction de systèmes de chiffrement par flux à très haut débit.

Dans une autre publication, P. Camion et A. Canteaut ont mis en évidence l'existence d'un compromis entre le degré de la forme algébrique normale et l'ordre de non-corrélation de toute fonction définie sur $\mathbf{F}_q$ et ont également contruit des familles infinies de fonctions t-résilientes de degré optimal. Ce résultat induit un nouveau critère de sécurité pour les primitives cryptographiques conventionnelles, tels les chiffrements à clef secrète, qui enrichit la notion de multipermutation introduite par Schnorr et Vaudenay (CRYPTO"96, [362]).

4 Actions industrielles

Ces actions se sont stabilisées cette année avec la signature du contrat DRET, la première année du contrat européen Aquarelle (voir §5.2.1) et l'extension de l'étude poursuivie avec l'entreprise COGENIT.

4.1 Théorie des codes et Mathématiques discrètes

Il s'agit d'une action de recherche fondamentale qui fait suite à l'étude intitulée *recherche mathématique et algorithmique en vue d'applications en cryptographie* — menée par M. MINOUX, conseiller scientifique à la DRET, en 93-94.

Un contrat a été signé en Avril 96, liant la DRET et l'INRIA (projet CODES), pour une étude de deux ans.

L'étude portera sur deux classes de codes *remarquables*, tant au niveau théorique qu'applicatif : les codes de Reed-Muller et les codes de Goppa.

4.2 Proposition ANVAR (COGENIT-CODES)

La collaboration avec la société COGENIT s'est poursuivie en 1996. L'essentiel a été la préparation et le dépot d'une proposition auprès de l'ANVAR.

Il s'agit de réaliser un *paquetage cryptographique*. Le logiciel proposé doit

- fournir la plupart des fonctionnalités usuelles, signature, controle d'accés, chiffrement ...

– proposer les primitives et les protocoles cryptographiques d'usage courant dans la communauté.

Sur cette action, l'INRIA a globalement un role d'expert. D'autres projets de Rocquencourt, dont le projet ALGO, doivent participer.

La proposition finale a été déposée à l'ANVAR en octobre 1996.

5 Actions nationales et internationales

5.1 Action nationales

Collaboration scientifique et échanges se sont poursuivis en 1996, 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 à cause de l'action des chercheurs extérieurs du projet issus de ces universités. Les chercheurs extérieurs sont tous habilités à diriger des recherches, 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'accroitre 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. C. Carlet et D. Le Brigand, qui résident à Paris, peuvent diriger des stages ou des thèses au projet (ainsi la thèse de G. Haché, dirigée par D. Le Brigand).

5.1.1 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 P. CHARPIN.

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. Une première réunion aura lieu à l'Ecole des Mines de Nantes les 18 et 19 Novembre 96. Ces journées sont organisées localement par G. Chassé. Une trentaine de participants et une quinzaine de conférences sont prévues.

Le projet entretient des relations suivies avec la DRET. Tous les membres du projet CODES participent activement au *séminaire de codage de la DRET*, qui a lieu une fois par mois. Le but de ces réunions est d'entretenir des échanges scientifiques entre les chercheurs et les ingénieurs, et aussi entre les représentants des secteurs publiques et industriels.

Le séminaire est organisé par Jean-marc Couveignes, pour la DRET, et par P. Charpin et S. Harari (pour la communauté des chercheurs).

Les autres séminaires auxquels participent régulièrement les membres du projet sont ceux de : l'ENST (G. Cohen), l'ENS-Ulm (J. Stern), le GECT de Toulon (J. Wolfmann), du département de mathématiques de Limoges (T. Berger) et l'INRIA (projet CODES).

5.1.2 Ecoles doctorales

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 les deux DEA parisiens :

- *Méthodes algébriques*, Paris 6, D. LE BRIGAND.
- *Algorithmique*, X-Ulm et universités Paris-centre. filière *Compléxité, codage et Cryptographie*, D. AUGOT, P. CHARPIN et N. SENDRIER.

Les étudiants en thèse assurent des cours ou travaux dirigés, dans des universités à titre de moniteur, ou dans des écoles d'ingénieur (ainsi G. Bommier au lycée Fenelon, A. Canteaut à l'ENSTA, C. Fontaine à l'Université Cergy-pontoise). Les chercheurs de 3ème cycle du projet sont généralement inscrits dans les formations doctorales de Paris 6. Ils sont associés à l'équipe de D. LAZARD (LITP, Calcul Formel et Algorithmique).

Jurys de thèse (fin 95-96) :

Novembre 95 Alexis BONNECAZE, Université de Nice.
Rapporteur : C. Carlet.

Janvier 96 Thierry BERGER, Habilitation, Université de Limoges.
Jury : P. Charpin et F. Laubie (co-direction), D. Le Brigand (rapporteur), P. Camion.

Mai 96 Sylvie JACQ, Université de Limoges.
Jury : T. Berger.

Septembre 96 Gaetan HACHÉ, Thèse d'Université de Paris VI.
Jury : D. Le Brigand (direction), P. Charpin, J. Wolfmann (rapporteur).

Octobre 96 Anne CANTEAUT, Thèse d'Université de Paris VI.
Jury : P. Camion (direction), C. Carlet, P. Charpin.

Octobre 96 Florent CHABAUD, Ecole Polytechnique.
Jury : P. Camion (rapporteur), P. Charpin.

Décembre 96 Guillaume PLANQUETTE, Université de Rennes 1.
Jury : P. Charpin.

5.2 Actions internationales

5.2.1 Relations Européennes

Le projet participe à AQUARELLE, consortium européen, managé par ERCIM, qui regroupe

- 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.

Aquarelle est un projet européen (section IE-2005) visant à homogénéiser les ressources culturelles actuellement existantes (tableaux, manuscrits ...). Ces ressources appartiennent aux institutions représentées par les différents partenaires culturels. Le but est 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" (ou vignettes), dont la valeur, bien que faible, n'est pas nulle.

Les partenaires culturels ont demandé que soit mise en place une protection de ces images. Le projet CODES intervient en proposant une protection basée 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. Cette équipe a déjà un algorithme de marquage d'image, sujet à améliorations, par exemple en utilisant des techniques de codage pour améliorer la résistance de la marque.

D'autre part, nous avons dégagé les fonctionalités que peut offrir un tel algorithme. Nous proposons de mettre en place un serveur de clés, qui transmet aux propriétaires des images des clés de marquage. Le protocole d'échange de clés repose sur la méthode de Diffie-Hellman, qui ne nécessite pas de canal sécurisé. 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 qu'il a stockée.

5.2.2 Invitations

Le projet a une politique d'invitation "large", au plan national et au plan internationale. Cette année, E.F. Assmus (USA), T. Ericson (Suède) et S. Lytsin (Israel) ont séjourné chacun un mois au projet.

D'autre part, le projet a accueilli, pour de courtes durées, en 1996 :

- Bernard Courteau (Université de Sherbrooke, Canada),
- James Massey (ETH-Zentrum, Suisse),
- Harold Mattson (Université de Syracuse, USA),
- Igor Shparlinski (Université de Macquarie, Australie).

6 Diffusion des résultats

6.1 Colloques et rencontres

Les résultats obtenus par les participants au projet sont largement diffusés, dans des séminaires nationaux, à l'étranger dans les séminaires des universités visitées et dans les colloques internationaux. D'autre part, le projet s'efforce de participer aux principaux colloques ou workshops portant sur ses thèmes de recherche.

Séjour courts dans des universités et laboratoires en 96 :

- A. Canteaut : Ecole Polytechnique de Zurich (invitée par J. Massey).
- P. Charpin : Université de Linkoping (invitée par T. Ericson), Université de Turku (invitée par A. Tietäväinen) et "St.Petersburg State Academy of Aerospace instrumentation"(invitée par S. Bezzateev).
- N. Sendrier : Université de Montréal (invité par C. Crépeau).

Participation à des Colloques fin 95-96 :

- *Colloque IEEE on Information Theory*, Whistler, Canada, 17-22 septembre 1995.
  Conférenciers : T. Berger, C. Carlet, P. Charpin, G. Haché.
  Participants : A. Canteaut, N. Sendrier.
- *Colloque Cryptographie*, CIRM Luminy, France, 25-29 septembre 1995.
  Conférencier invité : P. Camion.
- *Mediterranean Workshop on Coding and Information Integrity*, Palma de Majorque, Espagne, 28 février - 1er mars 1996.
  Conférenciers : A. Canteaut, C. Carlet, N. Sendrier.
  Participant : P. Charpin (membre du comité scientifique).
- *International Colloquium on Geometry, Algorithmes and Arithmetic in Error Correcting Codes*, Pointe à Pitre, Guadeloupe, 1er-5 avril 1996.
  Conférencier : G. Haché.
  Conférencier invité : D. Le Brigand.
- *EUROCRYPT'96*, Saragosse, Espagne, 12-16 mai 1996.
  Conférenciers : A. Canteaut, P. Camion.
- *Fifth International Workshop on Algebraic and Combinatorial Coding Theory ACCT'96*, Sozopol, Bulgarie, 1er-7 juin 1996.
  Conférenciers : T. Berger, G. Bommier, C. Carlet, P. Charpin.
- *The 2nd IMACS Conference on Applications of Computer Algebra*, Hagenberg, Autriche, 17-20 juillet 1996.
  Conférencier : D. Augot.
- *CRYPTO'96*, Santa-Barbara, USA, 18-22 août 1996.
  Conférenciers : A. Canteaut, P. Camion.
- *PRAGOCRYPT'96*, Prague, République Tchèque,
  30 septembre - 3 octobre 1996.
  Conférenciers : C. Carlet, C. Fontaine.
  Participants : P. Charpin, P. Camion.
- *Winter school on Coding and Information theory*, Molle, Suède,
  15-18 Décembre 1996.
  Conférencier : C. Fontaine.
  Participants : P. Charpin.

6.2 Contribution à un ouvrage sur la théorie des codes

P. Camion et P. Charpin sont tous deux auteurs d'un chapitre pour le *Handbook of coding theory*, ouvrage édité par V. Pless, W.C. Huffman et R.A. Brualdi.

P. Camion est chargé du chapitre intitulé *Codes and association schemes*. Une première version de 125 pages a été rédigée et est soumise à une communauté restreinte de chercheurs. Le texte sera repris sur la base des critiques récoltées.

P. Charpin est chargé du chapitre sur les codes cycliques, intitulé *Open problems on cyclic codes*.

6.3 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 Info. Theory*, *IEEE on Communications*, *Design, Codes and Cryptography*, *Journal of Cryptology*, *Finite Fields ...*

P. CAMION est éditeur des revues suivantes :

- Discrete Mathematics,
- Journal of Information and Optimisation Science (Analytic Publishing co., DELHI),
- Applicable Algebra in Engineering, Communication and Computing (AAECC), Springer Verlag,
- Design, Codes and Cryptography (Kluwer Academic Publishers),
- Cahiers du Centre d'Etudes de Recherche Opérationnelle (Univ. Libre de Bruxelles).

P. CHARPIN est éditeur de la revue Indienne : Journal of Combinatorics and Systems Sciences (JCISS) et expert pour la revue "Zentralblatt fur Mathematik".

7 Publications

Livres et monographies

[331] P. CAMION (réd.), *Codes and association schemes*, Handbook of Coding Theory, 1996. En préparation.

Thèses

[332] T. BERGER, *Groupes d'automorphismes et de permutations des codes affine-invariants*, Habilitation à diriger des recherches, Université Limoges, janvier 1996.

[333] A. CANTEAUT, *Attaques de cryptosystèmes à mots de poids faible et construction de fonctions t-résilientes*, thèse de doctorat, Université Paris 6, octobre 1996.

[334] G. HACHÉ, *Construction effective des codes géométriques*, thèse de doctorat, Université Paris 6, septembre 1996.

Articles et chapitres de livre

[335] D. AUGOT, P. CAMION, «On the computation of minimal polynomial, cyclic vectors and the Frobenius forms», *Linear Algebra and Its Applications*, 1996, A paraître.

[336] D. AUGOT, F. LEVY-DIT-VEHEL, «Bounds on the minimum distance of the duals of BCH codes», *IEEE Transaction on Information Theory 42*, 4, juillet 1996.

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

[338] T. BERGER, P. CHARPIN, «Groupe de permutations des codes affine-invariants», *Compte Rendus de l'Academie des Sciences de Paris t.321*, 1996, p. 1383–1387.

[339] T. BERGER, P. CHARPIN, «The permutation group of affine-invariant extended cyclic codes», *IEEE Transaction on Information Theory*, 1996, A paraître.

[340] T. BERGER, «On the automorphism groups of affine-invariant codes», *Designs Codes and Cryptography*, 7, 1996, p. 215–221.

[341] 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*, 1996, A paraître.

[342] C. CARLET, P. GUILLOT, «Une caractérisation des fonctions courbes», *Compte Rendus de l'Academie des Sciences de Paris*, 1995, A paraître.

[343] C. CARLET, P. GUILLOT, «A characterization of binary bent functions», *Journal of Combinatorial Theory, Series A*, 1996, A paraître.

[344] C. CARLET, «Generalized partial spreads», *IEEE Transaction on Information Theory 41*, 5, 1995, p. 1482–1487.

[345] C. CARLET, «On Z4-duality», *IEEE Transaction on Information Theory 41*, 5, 1995, p. 1487–1495.

[346] H. CHABANNE, «Factorizing of $x^n - 1$ and orthogonalization over finite fields of characteristic 2», *AAECC 6*, 1, 1995, p. 57–63.

[347] P. CHARPIN, V. ZINOVIEV, «On coset weight distributions of the 3-error-correcting BCH-codes», *SIAM Journal of Discrete Mathematics*, 1996, A paraître. Rapport INRIA N. 2828.

[348] P. CHARPIN, «Self-dual codes which are principal ideals of the group algebra $\mathbf{F}_2[\{\mathbf{F}_{2^m}, +\}]$», *The Journal of Statistical Planning and Inference Special volume : Affine Designs, Orthogonal Arrays and Related Topics*, 1996, A paraître. Rapport INRIA N. 2325.

[349] 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.

[350] F. LAUBIE, A. MOVAHHEDI, «Substitutions de séries formelles et cyclotomie», *Journal of Number Theory*, 58, 1996, p. 253–266.

[351] F. LAUBIE, M. SAÎNE, «Ramification of automorphisms of $k(t)$)», *Journal of Number Theory*, 1996, A paraître.

[352] D. LE BRIGAND, «Classification of algebraic function fields with divisor class number two», *Finite Fields and Their Applications*, 2, 1996, p. 153–172.

[353] D. LE BRIGAND, «Quadratic algebraic function fields with ideal class number two», *Arithmetic, Geometry and Coding Theory, W. de Gruyter*, 1996, p. 105–126.

[354] F. LEVY-DIT-VEHEL, S. LITSYN, «More on the covering radius of BCH codes», *IEEE Transaction on Information Theory 42*, 3, mai 1996.

[355] N. SENDRIER, «On the dimension of the hull», *SIAM Journal on Applied Mathematics*, 1996, A paraître.

Communications à des congrès, colloques, etc.

[356] D. AUGOT, F. FONTAINE, «Protection des droits et marquage d'image», *in : Electronic Imaging and The Visual Arts (EVA"96)*, Paris, France, décembre 1996.

[357] D. AUGOT, «Computing Groebner bases for finding codewords of small weight», *in : The 2nd IMACS Conference on Applications of Computer Algebra*, RISC Linz, Autriche, 17-20 juillet 1996.

[358] T. BERGER, P. CHARPIN, «Permutation group of some affine-invariant codes over extension fields», *in : Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-5)*, Sozopol, Bulgarie, 1-7 juin 1996.

[359] T. BERGER, «The automorphism group and the permutation group of affine-invariant codes», *in : Finite Fields and their Applications*, edited by S. Cohen H. Niederreiter (réd.), *London Math. Society, Lecture Note 233*, p. 32–45, 1996.

[360] F. BLANCHET, G. BOMMIER, «Quasi-cyclic Goppa codes», *in : Algebraic and Combinatorial Coding Theory*, *5*, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, UNICORN, p. 37–43, juin 1996.

[361] P. CAMION, A. CANTEAUT, «Construction of t-resilient functions over a finite alphabet», *in : Advances in Cryptology - EUROCRYPT'96*, U. Maurer (réd.), *Lecture Notes in Computer Science*, 1070, Springer-Verlag, p. 283–293, 1996.

[362] P. CAMION, A. CANTEAUT, «Generalization of Siegenthaler inequality and Schnorr-Vaudenay multi-permutations», *in : Advances in Cryptology - CRYPTO'96*, N. Koblitz (réd.), *Lecture Notes in Computer Science*, 1109, Springer-Verlag, p. 372–386, 1996.

[363] A. CANTEAUT, « A new algorithm for finding minimum-weight words in large linear codes », *in : Cryptography and Coding - 5th IMA Conference*, C. Boyd (réd.), *Lecture Notes in Computer Science*, 1025, Springer-Verlag, p. 205–212, 1995.

[364] A. CANTEAUT, « True minimum distance of some narrow-sense BCH codes of length 511 », *in : Mediterranean Workshop on Coding and Information Integrity*, Palma-de-Majorque, Espagne, février 1996.

[365] C. CARLET, « A characterization of binary bent functions », *in : Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-5)*, Sozopol, Bulgarie, 1-7 juin 1996.

[366] C. CARLET, « A construction of bent functions », *in : Finite Fields and their Applications*, edited by S. Cohen H. Niederreiter (réd.), *London Math. Society, Lecture Note 233*, 1996.

[367] C. CARLET, « Hyper-bent functions », *in : Mediterranean Workshop on Coding and Information Integrity*, Palma-de-Majorque, Espagne, février 1996.

[368] C. CARLET, « Hyperbent functions », *in : Actes de Pragocrypt'96, Czech Technical University Publishing House*, p. 145–155, Prague, 1996.

[369] P. CHARPIN, A. TIETAVAINEN, V. ZINOVIEV, « On binary cyclic codes with minimum distance three », *in : Fifth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-5)*, Sozopol, Bulgarie, 1-7 juin 1996.

[370] C. FONTAINE, « The nonlinearity of a class of boolean functions with short representation », *in : Actes de Pragocrypt'96, Czech Technical University Publishing House*, p. 129–144, Prague, 1996.

[371] G. HACHÉ, « Computation in algebraic function fields for effective construction of algebraic geometric codes », *in : AAECC 11*, *Lecture Notes in Computer Science*, 948, Springer-Verlag, p. 283–293, 1996.

[372] G. HACHÉ, « PAFF: An axiom package for algebraic function field in one variable », *in : Geometry, Algorithmic and Arithmetic in the Theory of Error Correcting Codes*, Pointe à Pitre, Guadeloupe, 1-5 avril 1996.

[373] D. LE BRIGAND, « Class-numbers in function fields: historic point of view and an open problem », *in : Geometry, Algorithmic and Arithmetic in the Theory of Error Correcting Codes*, Pointe à Pitre, Guadeloupe, 1-5 avril 1996.

[374] N. SENDRIER, « Efficient generation of binary words of given weight », *in : Cryptography and Coding - 5th IMA Conference*, C. Boyd (réd.), *Lecture Notes in Computer Science*, 1025, Springer-Verlag, p. 184–187, 1995.

Rapports de recherche et publications internes

[375] P. CAMION, A. CANTEAUT, « Construction of t-resilient functions over a finite alphabet », *rapport de recherche n°RR-2789*, INRIA, février 1996.

[376] 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 », *rapport de recherche n°RR-2685*, INRIA, octobre 1995.

[377] P. CHARPIN, V. ZINOVIEV, « On coset weight distributions of the 3-error-correcting BCH-codes », *rapport de recherche n°RR-2828*, INRIA, mars 1996.

[378] P. CHARPIN, « Tools for coset weight enumerators of some codes », *rapport de recherche n°RR-2640*, INRIA, août 1995.

[379] F. LAUBIE, « Introduction to the theory of Nim-linear codes », *rapport de recherche n°RR-2736*, INRIA, novembre 1995.

[380] N. SENDRIER, « Un algorithme pour trouver la permutation entre deux codes binaires équivalents », *Rapport de Recherche n°2853*, INRIA, Avril 1996.

[381] V. ZINOVIEV, « On the solution of equations of degree ≤ 10 over finite fields $GF(2^m)$ », *rapport de recherche n°RR-2829*, INRIA, janvier 1996.

Divers

[382] E. ASSMUS, «Linearly derived Steiner triple systems», 1995, Soumis pour publication.

[383] P. CHARPIN, A. TIETAVAINEN, V. ZINOVIEV, «On binary cyclic codes with $d = 3$», 1996, Soumis pour publication.

[384] F. LAUBIE, «Linear ternary Greedy codes», 1996, Soumis pour publication.

[385] F. LAUBIE, «Ramification des polynômes de Chebyshev», 1996, Soumis pour publication.

[386] N. SENDRIER, «On the structure of a randomly permuted concatenated code», Soumis pour publication.

8 Abstract

The research area of the CODES project is Coding and Cryptography. The project has however a double aim: developing fundamental research in Coding Theory as well as placing oneself intentionally in the area Applications to "Protecting Information".

By and large, the studies we are concerned with provide conditions for practical applications of error-correcting coding for transmission and storage of data in modern telecommunication and data storage systems. They include investigations of potential areas of coding applications and of the ways of providing high error-correcting capacity under random and specific noise.