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 [AJT]

Personnel INRIA
Daniel Augot [CR]
Anne Canteaut [CR]
Jean-Pierre Tillich [en délégation de l'Université d'Orsay]

Conseiller scientifique
Guy Chassé [École des Mines de Nantes]

Collaborateurs extérieurs
Thierry Berger [Université Limoges]
Francis Blanchet [Lycée Montaigne]
Claude Carlet [Université Paris 8]
Éric Filiol [ESAT]
Caroline Fontaine [Université Lille]
Philippe Gaborit [Université Limoges]
Françoise Levy-dit-Vehel [ENSTA]
Pierre Loidreau [ENSTA]

Doctorants
Magali Bardet-Turel [AMN]
Harold Ollivier [X-Telecom]
Matthieu Finiasz [AMN]
Fabien Galand [Bourse BDI]
Ludovic Perret [Bourse MESR]
Carmen Nedeloaia [Bourse régionale]
Gregory Olocco [Bourse MESR]
Emmanuel Prouff [ATER Orsay]
Michael Quisquater [Katholieke Universiteit Leuven, Belgique]
Cédric Tavernier [Bourse DGA]
Marion Videau [Bourse DGA]

Stagiaires
Raghav Bhaskar [Stage Égide, Indian Institute of Technology, Delhi, de septembre à décembre 2002]
Xavier Dahan [Stage de fin d'études, Université de Versailles, de juillet à août 2002]
Ludovic Perret [Stage de DEA, Université d'Évry, de février à juin 2002]
Philippe Quanty [Stage de DEA, Université de Limoges, d'avril à juin 2002]

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. 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 mêlent 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, Niederreiter, 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 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] 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.

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

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 ...), génération d'aléa ;
4. Algorithmes de décodage (correction d'erreurs et cryptanalyse) ;
5. Protection des droits d'auteurs (marquage des images et des films numérisés).

6. Résultats nouveaux

6.1. 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 ...

6.1.1. Groupes d'automorphismes

Participants : Thierry Berger, Francis Blanchet.

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. C'est un axe traditionnel du projet codes.

Cette année. T. Berger s'est intéressé aux codes basés sur le métrique « rang », différente de la métrique de Hamming usuellement considérée. Pour cette métrique il a défini la notion d'isomorphisme et étudié les isométries de codes de Gabidulin et des codes hyperboliques. Il a montré que leur groupe de permutations est trivial.

6.1.2. Codes cycliques et codes auto-duaux

Participants : Carmen Nedeloaia, Pascale Charpin, Philippe Gaborit.

Carmen Nedeloaia s'est particulièrement intéressée à l'étude des codes cycliques à racines multiples, notamment les codes cycliques auto-duaux. En utilisant une construction du type $|u|u+v|$ itérée, elle a réussi à montrer que tout code cyclique à racines multiples admet une *construction quadratique* (« squaring construction »). Cette construction, ainsi que l'utilisation du *code shadow* a facilité le calcul des énumérateurs des poids, qui ont été obtenus pour tous les codes cycliques auto-duaux de longueur plus petite ou égale à 120, à 4 exceptions près [68].

Philippe Gaborit a étudié de nouveaux codes auto-duaux construits de deux méthodes différentes, la première généralise la construction des codes quadratiques doublement circulant [29][32], la deuxième méthode est inspirée de construction de la famille des codes dits CORTEX [31]. Ces deux méthodes ont permis entre autres de construire des codes avec des paramètres non-connus avant : un code [92,46,16] sur GF(2), un code [52,26,15] sur GF(3) ou encore un code [46,23,14] sur GF(4).

Il a étudié de nouveaux designs contenus dans certains codes auto-duaux, en particulier on montre dans [14], l'existence de 1-designs ou 2-designs inconnus auparavant dans certains codes s-extrémaux ayant la particularité d'avoir une ombre longue. Philppe Gaborit a construit un algorithme de décodage élémentaire et « à la main » du code RM(2,5) simplement à partir d'une description combinatoire de ses éléments [30].

Du point de vue combinatoire il a construit de nouveaux réseaux unimodulaires en dimensions supérieures à la dimension à partir de codes auto-duaux et de la construction A ou à partir d'une construction par voisinage [28], en particulier on construit le premier réseau unimodulaire de norme 6 en dimension 60 dont on donne la série theta. On étudie aussi dans [40] des réseaux construits à partir de codes sur l'anneau F3+vF3.

6.1.3. Codes de Goppa

Participant : Matthieu Finiasz.

Les codes de Goppa ont une distribution de poids proche d'une distribution binomiale. Ceci a déjà été prouvé pour les poids moyens. En revanche pour les petits poids rien n'est certain.

En utilisant un algorithme proche de celui utilisé pour la signature on peut trouver (au bout d'un grand nombre d'essais) des mots de poids faible. En répétant l'expérience un grand nombre de fois on peut ainsi faire des statistiques sur le nombre moyen d'essais et ainsi on arrive à determiner expérimentalement la distribution des petits poids. On constate que là encore tout ce passe comme si on était très proche d'une distribution binomiale.

Ce résultat est interessant car il permet de déterminer la compléxité de notre algorithme pour trouver des mots de poids minimum est d'ainsi choisir des paramètres qui permettent de trouver de tels mots facilement, tout en rendant cette tâche difficile pour quelqu'un d'extérieur. Ceci nous donne donc une base fiable pour essayer de construire de nouveaux cryptosystèmes basés sur les codes correcteurs d'erreurs.

6.2. Cryptographie à clé publique

6.2.1. Système de chiffrement utilisant des codes correcteurs

Participants : Daniel Augot, Thierry Berger, Pierre Loidreau, Nicolas Sendrier, Matthieu Finiasz.

Dans ce thème sont regroupées l'étude et la conception de systèmes de chiffrement 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.

En 2002, Pierre Loidreau a poursuivi son travail de recherche en continuation de sa thèse. Il s'est intéressé notamment au développement d'algorithmes de chiffrement à clé publique fondés sur le problème de décodage en métrique rang. Initialement proposés par Gabidulin, ces systèmes de chiffrement permettent l'utilisation de clé de taille moindre que pour leur équivalent, le système de McEliece en métrique de Hamming. En 2001, avec Thierry Berger de l'université de Limoges, il a proposé l'utilisation de sous-codes de codes de Gabidulin pour masquer la structure importante de ces codes, les seuls utilisés dans ces systèmes. Ils ont étudié la résistance du système aux différentes attaques connues. Ils ont également montré que cette approche pouvait être étendue au cas de la métrique de Hamming, et permettait de réduire de façon significative la taille des clés, à sécurité constante. Actuellement Pierre Loidreau s'intéresse à la structure des codes de Gabidulin, notamment aux sous-codes trace et aux sous codes-additifs. Il a également encadré un étudiant de l'ENSTA qui à implanté un algorithme de décodage des codes de Gabidulin, en langage C au moyen de la bibliothèque de calcul ZEN.

Matthieu Finiasz et Daniel Augot ont inventé un nouveau système de chiffrement à clé publique, basé sur la difficulté de reconstruire un polynôme d'aprés ses valeurs « bruitées ». Ce système présente des clés plus courte que le système de MacEliece, mais les blocs de chiffrements sont beaucoup plus longs. Reste à établir la solidité de ce système. Ce système a été soumis à la conférence Eurocrypt à Varsovie [42].

Nicolas passé a obtenu son habilitation à diriger des recherches en rédigeant un mémoire sur la cryptographie à clé publique basée sur les codes correcteurs d'erreurs [13].

6.2.2. Cryptosystèmes basés sur des problèmes combinatoires

Participants : Françoise Levy-dit-Vehel, Pierre Loidreau.

L'activité de Françoise Levy-dit-Vehel et de Pierre Loidreau se concentre autour de l'ACI ACCES. Françoise Levy-dit-Vehel étudie des méthodes de construction de cryptosystèmes à clef publique basés sur des problèmes difficiles de combinatoires. Dans ce cadre, le premier problème étudié a été celui de la satisfaisabilité des ensemble de clauses à trois littéraux (3-sat). Ce travail a fait l'objet d'un rapport interne ENSTA [ref], en collaboration avec Ludovic Perret.

Le recrutement de Ludovic Perret en thèse (septembre 2002) oriente à présent l'activité vers la recherche de « bons » problèmes difficiles, c'est-à-dire pour lesquels on peut prouver des résultats de complexité en

moyenne tels que : ces problèmes sont dans la classe RNP ou RNPC[3]. Ludovic Perret explore la possibilité d'exhiber des classes d'instances particulières de 3-sat qui pourraient avoir cette propriété. Parallèlement, Françoise Levy-dit-Vehel et Ludovic Perret cherchent à adapter au contexte cryptographique des problèmes RNPC connus.
Un autre aspect du travail concerne la robustesse d'un schéma cryptographique basé sur de tels problèmes vis-à-vis des attaques destinées à récupérer le clair correspondant à un chiffré particulier. La clef publique et le chiffré étant des polynômes multivariés sur un corps fini, ces attaques exploitent l'existence de termes dits « isolés » dans la clef publique, dont la présence dans le chiffré dévoile de l'information sur le clair. De telles attaques sont en général relativement efficaces sur ce type de systèmes, et la construction d'une clef publique résistante à celles-ci reste un problème ouvert. Les chercheurs impliqués ont initié une collaboration avec les membre de l'ACI POLYCRYPT.

6.2.3. Cryptosystèmes basés sur des problèmes algébriques

Participants : Daniel Augot, Magali Bardet, Philippe Gaborit.

Daniel Augot encadre Magali Bardet qui est codirigée par Jean-Charles Faugère du LIP6, spécialiste de la résolution de systèmes d'équations algébriques. L'axe de recherche ici étudié est la cryptanalysee de HFE. Jean-Charles Faugère a réussi à casser le challenge HFE proposé, en moins de 96 heures. Il a pu mener ce calcul en constatant expérimentalement que les systèmes algébriques « HFE » ne sont des pas systèmes aléatoires.

Magali Bardet (avec Bruno Saly et Jean-Charles Faugère) a étudié la complexité de la résolution d'un système d'équations algébriques aléatoires. En utilisant des techniques de développements asymptotiques d'intégrales, on peut obtenir des bornes de complexité théorique très précises pour les systèmes algébriques aléatoires dans un corps fini. En particulier, on obtient l'équivalent sur les corps finis de la borne $1 + (d_1 - 1) + \ldots + (d_m - 1)$ (Lazard 83) pour des systèmes de m polynomes de degre d_i sur le corps des rationnels.

Ces bornes théoriques sont particulièrement utiles pour faire la distinction en pratique entre un système aléatoire (difficile) et un système provenant d'un problème cryptographique comme HFE (plus facile).

D'autre part, Philippe Gaborit et Patrick Solé ont proposé un nouveau système CTRU de chiffrement utilisant des polynômes et proche du cryptosystème NTRU. Le système est fondé sur l'utilisation de polynomes à deux variables que l'on considére suivant les cas, modulo des polynomes à une variable et de degré differents. Le systeme obtenu a des performances similaires à celles du systeme NTRU , tout en ayant une preuve beaucoup plus simple. Un rapport de recherche a été publié par l'INRIA [81], mais le système a hélas été cassé.

6.2.4. Signature par le « Extended Domain Hash »

Participant : Matthieu Finiasz.

La plupart des systèmes de signatures actuels utilisent la même méthode : on hache le document à signer en une chaine de bits de la bonne longueur et on y applique une fonction à sens unique. C'est ce que l'on appelle le FDH (Full Domain Hash) du fait que l'on hache le document en une chaine aléatoire qui peut prendre n'importe quelle valeur de l'ensemble de définition de la fonction à sens unique. Dans le cas de la signature avec McElliece, Matthieu Finiasz a introduit le « Extended Domain Hash » : le hachage donne lui aussi une chaine de bits, mais ce coup ci elle prend une valeur aléatoire dans un ensemble plus grand que le domaine de définition de notre fonction à sens unique. Cela singifie que l'on ne peut appliquer cette fonction qu'à certains hachés. On ajoute donc un compteur au document et on le hache avec le document, jusqu'à trouver un haché valide. Cette méthode a été baptisé XDH (eXtended Domain Hash) et il doit aussi être possible de prouver sa sécurité.

6.2.5. Sécurisation d'applications partagées

Participants : Daniel Augot, Raghav Bhaskar.

[3] Randomized NP problems, randomized NP-complete problems.

Raghav Bhaskar, étudiant de l'Indian Institute of Technology, est venu effectuer un stage de quatre mois au projet codes, coencadré par V. Issarny (Projet Arles), et suite à ce stage il effectuera une thèse sous la direction de V. Issarny et coencadré par Daniel Augot. L'objectif de ce travail est de proposer des solutions cryptographiques aux problèmes de sécurité posés pour les environnements distribués sans fil. En effet ces environnements (PDAs par exemple) sont trés sujet aux attaques par écoute radio, il faut alors sécuriser les communications. Dans le cadre de son stage R. Baskar a étudié la solution de sécurité proposée par le projet Arles dans le cadre du scénario AdHocFS (partage de fichiers), et a montré les problèmes inhérents à cette proposition. L'emploi de protocoles cryptographiques plus évolués, notamment les protocoles de mise en accord de clé multi-utilisateur (généralisations du protocole de Diffie-Hellman bien connu) permet d'obtenir la sécurité demandée.

R. Baskar continuera ces travaux dans le cadre de sa thèse, en les généralisant à d'autres propblèmes de sécurité rencontrés dans d'autres applications. Cette action permet d'établir une collaboration avec Arles, et aussi avec Hipercom.

6.3. Algorithmes de décodage

Participants : Daniel Augot, Anne Canteaut, Grégory Olocco, Lancelot Pecquet, Magali Bardet-Turel.

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. La troisième est l'émergence de techniques de décodage dits itératifs, de bonne performance, mais difficiles à justifier théoriquement.

Grégory Olocco et Jean-Pierre Tillich s'intéressent aux apports des techniques de décodage itératif dans le domaine des codes correcteurs d'erreur. L'intérêt de ce type de décodage est qu'il approxime remarquablement le décodage optimal au maximum de vraisemblance pour une très large classe de codes, et reste de complexité algorithmique tout à fait raisonnable. Nous avons commencé par étudier, dans le cadre d'un contrat entre le CCETT et l'INRIA, le décodage itératif d'une nouvelle famille de codes brevetés par le CCETT, les codes cortex, et nous avons montré par une analyse théorique, comment choisir les paramètres de ces codes afin d'optimiser les performances du décodage itératif.

Une étude plus poussée de ces codes a par ailleurs montré que la plupart de ces codes ont des performances analogues à celles des codes aléatoires (qui sont à peu de choses près optimaux), lorsqu'ils sont décodés au maximum de vraisemblance. C'est la première fois qu'une telle propriété est montrée pour une famille particulière de codes auto-duaux. Il est probable que cette famille de codes donne pour des longueurs petites ou moyennes des codes performants avec une complexité de décodage acceptable.

Par ailleurs, depuis deux ans Jean-Pierre Tillich s'intéresse avec Gilles Zémor à l'utilisation de techniques isopérimetriques ou/et de concentration de la mesure en probabilité pour estimer les probabilités d'erreur après décodage de codes correcteurs d'erreur. Cette grandeur est jugée fondamentale par les ingénieurs pour évaluer les performances d'un code, mais est malheureusement très délicate à estimer.

L étude de cette quantité a été débutée sur deux modèles simples de canaux d'erreur : le canal à effacement (qui est un modèle simplifié d'Internet) et le canal binaire symétrique (qui modélise un bruit gaussien suivi d'une quantification). L'approche est d'estimer cette probabilité d'erreur en fonction de paramètres du code qui sont assez souvent connus comme la distance minimale, ou assez faciles à estimer comme le seuil critique qui est la valeur du bruit pour lequel le décodage echoue avec probabilité 1/2. Les premiers résultats indiquent que lorsque ces codes sont décodés au maximum de vraisemblance, cette grandeur décroit exponentiellement avec la distance minimale, et ce tant que le paramètre de bruit inférieur au seuil critique moins une constante positive arbitrairement petite. C'est la première fois qu'une telle borne est obtenue, et la dépendance exponentielle ne peut être améliorée.

Enfin plus récemment, le modèle d'erreur continu le plus populaire a été étudié : le canal gaussien, et là aussi il a été montré que la probabilité d'erreur décroit exponentiellement avec la distance minimale du code. Ce travail va été présenté à la conférence ISIT en juillet, et la version journal a été soumise à *IEEE Transactions*

on Information Theory. Il est très probable que ces résultats s'étendent à un autre modèle populaire de canal d'erreur : le canal à évanouissement. Une autre extension de ce travail serait d'étudier avec ces techniques ce qui se passe quand un algorithme de décodage suboptimal est utilisé (comme le décodage itératif).

Par ailleurs Jean-Pierre Tillich et Joël Friedman ont étudié le vieux problème qui est de trouver des bornes supérieures sur la distance minimale d'un code correcteur d'erreur de rendement donné. Leur approche du problème est entièrement nouvelle et consiste a relier ce problème à l'estimation d'une quantité intervenant dans des problèmes isopérimetriques sur le cube discret. En développant des techniques pour borner supérieurement cette quantité ils ont retrouvé la meilleure borne sur la distance minimale connue à ce jour. Précisons que cette dernière borne n'a pas été améliorée depuis 30 ans (bien que de nombreux auteurs conjecturent fortement que cette borne devrait pouvoir être améliorée).

Décodage de codes de Reed et Muller : dans le but d'applications cryptographiques, Cédric Tavernier essaye d'améliorer un algorithme du a Goldreich, Rubinfeld et Sudan qui permet de décoder ces codes. Cet algorithme ne fonctionne pas quand le corps est trop petit, notamment dans le cas binaire qui est le plus important en pratique. Cédric Tavernier essaye de mélanger cette approche avec celle de Dumer, qui construit un décodage récursif des codes de Reed-Muller. L'objectif est de pouvoir décoder au delà de la distance minimale.

Dans un autre contexte, mais dans un problématique relative au codage, Thierry Berger étudie l'utilisation de codes pour prolonger la longueur de corrélation des systèmes d'étalement de spectre à débit constant. Le but est de démontrer les avantages des suites de corrélation multi-niveau par rapport aux suites binaires utilisées actuellement dans ce contexte

6.4. Décodage et cryptanalyse

Participants : Daniel Augot, Anne Canteaut, Grégory Olocco, Cédric Tavernier.

6.4.1. Chiffrement à flot

Suite à de nombreux travaux récents, il est bien connu que les algorithmes de décodage sont des outils performants en cryptanalyse. Ainsi les techniques de décodage s'appliquent également à la cryptanalyse de tous les *systèmes de chiffrement à flot* qui utilisent des générateurs pseudo-aléatoires composés de registres à décalage à rétroaction linéaire. Un système de chiffrement à flot consiste à additionner bit à bit au message clair une suite binaire pseudo-aléatoire de même longueur, appelée suite chiffrante. Ce procédé est très utilisé car il est extrêmement rapide et, contrairement aux autres systèmes à clef secrète, il est très peu sensible aux erreurs qui pourraient survenir au cours de la transmission. La plupart des générateurs pseudo-aléatoires utilisés pour produire une suite chiffrante sont constitués de plusieurs registres à décalage à rétroaction linéaire, qui peuvent être combinés de différentes manières. La clef secrète du système correspond aux initialisations des différents registres.

Pour retrouver ces initialisations, une méthode classique, introduite par Siegenthaler en 1985, consiste à exploiter l'existence d'une éventuelle corrélation entre la sortie du générateur pseudo-aléatoire et celle d'un des registres à décalage employés. Il suffit alors d'essayer toutes les initialisations pour cet unique registre et de comparer les suites ainsi obtenues à quelques bits de la suite chiffrante ; l'observation d'un pic de corrélation permet alors de détecter l'initialisation effectivement utilisée. Toutefois, la complexité de cet algorithme est exponentielle en la longueur du registre à décalage examiné. La cryptanalyse devient donc hors de portée dès lors que la taille des registres dépasse 50 ou 60.

Pour éviter de passer en revue toutes les initialisations, on assimile alors la recherche de l'initialisation d'un registre à un problème de correction d'erreurs : on considère que la suite chiffrante résulte de la transmission de la suite produite par un seul registre à travers un canal bruité. La suite générée par un seul registre étant fortement redondante (il s'agit d'une suite engendrée par une relation de récurrence linéaire), on peut la reconstituer à l'aide d'un algorithme de décodage. L'efficacité de cette attaque, appelée *attaque par corrélation rapide*, dépend donc des performances du code correcteur utilisé pour représenter le système.

Anne Canteaut a conçu, avec M. Trabbia une nouvelle technique d'attaque par corrélation rapide, fondée sur l'algorithme de décodage itératif de Gallager pour des équations de parité de poids 4 ou 5 . Cette attaque peut s'appliquer à des registres de grande taille, puisque le nombre de bits nécessaires à la cryptanalyse est

exponentiel en $L/(d-1)$ où d est le poids des équations utilisées, alors qu'il était exponentiel en $L/2$ dans toutes les attaques précédentes. Elle est par ailleurs extrêmement rapide : ainsi, retrouver l'initialisation d'un registre de longueur 40 en présence de 30 % d'erreurs nécessite la connaissance de 9700 bits de la suite chiffrante et un temps de calcul moyen d'une dizaine de secondes.

6.4.2. Chiffrement par bloc

Cédric Tavernier et Daniel Augot s'intéresse à l'approximation d'une fonction de chiffrement par une fonction plus simple, par exemple un polynôme de petit degré. Le point de départ de ces travaux est l'article de T. Jakobsen où il cryptanalyse l'algorithme de Knudsen et Nyberg, en utilisant l'algorithme de décodage de Sudan. Cette attaque semble difficile à généraliser pour d'autres fonctions de chiffrement (eg DES, AES...), et les travaux restent en cours sur ce sujet.

6.5. Primitives du chiffrement symétrique

6.5.1. Fonctions booléennes

Participants : Claude Carlet, Pascale Charpin.

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. Elles 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*.

C. Carlet avec Y. Tarannikov ont montré que les critères de non-corrélation et de résilience peuvent être caractérisés par l'existence de certaines séquences couvrantes. De plus, en considérant des séquences couvrantes particulières, ils ont exhibé des sous-classes de fonctions résilientes aux propriétés de non-linéarité intéressantes (article paru dans la revue Designs, Codes and Cryptography). C. Carlet avec Palash Sarkar a obtenu une nouvelle preuve de la borne de divisibilité et de la borne supérieure sur la non-linéarité des fonctions résilientes qu'il avait montrée en utilisant la forme numérique normale. Cette nouvelle preuve est basée sur les seules propriétés de la transformée de Fourier (un article paru dans la revue Finite fields and Applications).

Dans son article à paraître dans la sélection des meilleurs articles présentés à la conférence Fq6 (publiée par Springer Verlag), C. Carlet a montré que presque toutes les fonctions booléennes sont de haute complexité vis à vis de plusieurs critères tels que la nonlinéarité, le nombre minimal de termes dans les formes algébriques normales des fonctions équivalentes, le degré algébrique et la non-normalité. La construction générale de fonctions courbes et résilientes connue sous le nom de Maiorana McFarland est malheureusement la seule connue qui permette de construire en nombres importants des fonctions courbes ou des fonctions résilientes présentant d'autres qualités cryptographiques telles qu'une bonne non-linéarité. Les fonctions ainsi construites sont des concaténations de fonctions affines. C. Carlet a obtenu une borne supérieure efficace sur la nonlinéarité de ces fonctions et a mis en évidence divers paramètres qu'elles permettent d'obtenir. Il a également montré qu'il est possible d'obtenir des résultats similaires et parfois meilleurs en concaténant des fonctions quadratiques. Ce travail a été présenté à CRYPTO 2002 et publié dans ses actes.

C. Carlet, avec Andrew Klapper a mis en évidence deux bornes supérieures sur les nombres de fonctions courbes et résilientes. Ce travail, présenté au congrès « 23rd Symposium on INFORMATION THEORY in the BENELUX » fait l'objet d'un article de 15 pages à paraître dans la « Special Issue » de Lecture Notes (Springer-Verlag) dédiée à Philippe Delsarte (Editeurs R. Calderbank et J.-J. Quisquater). Il a ensuite amélioré cette borne pour certains ordres de fonctions résilientes, dans un article en commun avec Aline Gouget, accepté pour présentation à Asiacrypt 2002 avec publication dans ses actes. Avec Cunsheng Ding, il a rédigé un article

résumant et généralisant l'état de l'art en matière de non linéarité parfaite des fonctions définies et à valeurs dans des groupes abéliens (article de 44 pages soumis à SIAM Journal on Discrete Mathematics).

Les travaux de Pascale Charpin se situent en amont et concernent :
- *Les propriétés descendantes des fonctions courbes*[4] (voir (3) et (6) avec Canteaut). L'idée générale de ce travail est d'introduire un élément de classification des fonctions courbes par le biais de leurs décompositions. Ce point de vue semble pertinent compte tenu de nos premiers résultats sur les décompositions par rapport aux espaces de codimension 2 : une grande diversité apparait qui n'est pas dans le cadre des classes établies.
- *Les propriétés de propagation des fonctions booléennes résilientes.* L'objet de ce travail (avec Pasalic (2) et (5)) est d'abord une meilleure compréhension de ces propriétés. D'un point de vue cryptographique, un critère de propagation évalue l'impact en *sortie* d'une perturbation de l'*entrée*. Le critère de résilience, lui, répond à une famille d'attaques *par corrélation* sur certains systèmes de chiffrement. Nous introduisons d'abord une nouvelle borne concernant la nonlinéarité des fonctions résilientes, borne qui prend en compte le degré de la fonction et certains critères de propagation. D'autre part, nous montrons que l'ordre de résilience induit des propriétés de divisibilité pour les dérivées, celles-ci pouvant être renforcées par le degré de propagation. Ainsi nous caractérisons une large famille de fonctions hautement résilientes ayant des structures linéaires. Nous montrons aussi, par ces bornes, l'influence du degré de la fonction dans l'établissement de bons compromis.

6.5.2. Primitive du chiffrement à flot

Participant : Thierry Berger.

Thierry Berger a étudié la génération de suites pseudo-aléatoires par des fractions 2-adique (Feedback with Carry Shift Register), similaire aux générateurs linéaires classiques sans retenue (Linear Feedback Shift Register). Il a analysé le recouvrement de structure de telles suites. Il a combiné les deux systèmes en utilisant un générateur LFSR et un générateur FCSR en série. C'est un travail commun avec F. Arnault et A. Necer (Limoges).

6.6. Chiffrement symétrique : cryptanalyse

Participants : Anne Canteaut, Éric Filiol, Marion Videau, Daniel Augot, Cédric Tavernier.

6.6.1. Cryptanalyse des chiffrements par blocs

Dans un algorithme de chiffrement par blocs, le choix de la fonction de substitution (correspondant aux boîtes-S du DES) est d'une extrême importance car il conditionne la résistance du système aux attaques classiques (cryptanalyses différentielle et linéaire). Il s'agit ici de fonctions vectorielles possédant le même nombre de bits en entrée et en sortie. Les fonctions dites presque courbes, qui sont celles qui assurent une résistance maximale aux attaques classiques, ont fait l'objet de nombreux travaux du projet CODES. Nous avons notamment donné de nouvelles caractérisations de cette propriété qui ont permis de construire de nouvelles fonctions presque courbes (*cf* [50]).

Toutefois, la résistance aux cryptanalyses linéaire et différentielle ne suffit évidemment pas à assurer la solidité d'un algorithme. Certains systèmes de chiffrement présentent ainsi des faiblesses particulières qui les rendent vulnérables à d'autres types d'attaques. Dans ce contexte, Anne Canteaut et Marion Videau se sont récemment intéressées aux critères de résistance liés à la cryptanalyse différentielle d'ordre supérieur. Cette attaque, introduite par Lai et Knudsen en 1994, exploite l'existence d'un biais statistique dans la distribution des dérivées d'ordre supérieur de la fonction itérée. Elle s'applique notamment lorsque le degré multivarié de la fonction de chiffrement est petit. Mais, la détermination de ce degré est un problème difficile dans la pratique puisqu'elle nécessite une étude précise de l'évolution du degré au cours des itérations successives de la fonction de tour. C'est pourquoi le champ d'application de cette attaque était jusqu'à présent réduit aux systèmes utilisant une fonction itérée de petit degré. Anne Canteaut et Marion Videau ont alors montré que le degré de deux itérations d'une fonction était étroitement lié à la divisibilité de ses coefficients de Fourier. Cette étude les a notamment conduit à exhiber une attaque différentielle d'ordre supérieur très générale sur les chiffrements de Feistel utilisant une fonction itérée de non-linéarité optimale. Elle leur a

[4] *i.e.,* définition de fonctions ayant de *bonnes* propriétés cryptographiques par décomposition de fonctions courbes

également permis de comprendre l'origine d'une attaque sur l'algorithme MISTY1, dont une variante est utilisée pour assurer la confidentialité des communications pour les mobiles de troisième génération. Ces travaux ont montré que, paradoxalement, la vulnérabilité de MISTY1 aux attaques différentielles d'ordre supérieur résultait directement de l'utilisation de fonctions presque courbes, alors que celles-ci garantissent une résistance optimale aux attaques différentielles et linéaires. Cette étude a conduit à formuler un nouveau critère de sécurité pour les chiffrements itératifs par blocs impliquant le spectre de Fourier de la fonction itérée. Il apparaît alors que la fonction inverse dans un corps fini d'ordre 2^{2n}, qui a été choisie pour l'AES, est la seule fonction connue qui assure simultanément une résistance optimale aux attaques différentielles et linéaires, et aux attaques différentielles d'ordre supérieur. L'ensemble de ces résultats fait l'objet d'un article à la conférence EUROCRYPT 2002 [52].

6.6.2. Attaques considérant la forme algébrique normale

L'attaque des systèmes de chiffrement symétriques, essentiellement basée sur une approche combinatoire qui permet de trouver une information de nature plus qualitative que quantitative. L'angle priviliégié par Eric Filiol est notammant de modéliser ces systèmes par un ensemble de fonctions booléennes et de trouver des structures biaisées dans leur forme algébrique normale (c'est-à-dire des polynômes multivariés où les bits de clef sont les variables). Ces structures peuvent alors être traduite de sorte à retrouver « facilement » des bits d'information sur la clef. Les résultats obtenus sont très prometteurs et ont fait l'objet d'une soumission à FSE 2003.

6.6.3. Testeurs

Cédric Tavernier manipule des « testeurs » pour des programmes calculant des pôlynomes sur un corps fini. La construction des testeurs fait intervenir des codes de Reed-Solomon et les propriétés métriques de l'espace de Hamming. Il faut donc réinterpréter les résultats en termes concrets, et dans le language des codes correcteurs et de la cryptographie. On va supposer dans la suite que l'on travaille sur un corps fini du type F_{2^n} que l'on notera par commodité F_q. On dispose d'une boite noire que l'on peut modéliser comme une fonction $f : F_q \longrightarrow F_q$. On suppose que l'on ne connait qu'une fraction des images de cette fonction et que les antécédants de ces images sont des points particuliers qui sont qualifiés de « points à espacement régulier ». On désire alors répondre à la question suivante : f est elle $O\left(\frac{1}{(d+2)^2}\right)$ proche d'un polynôme univarié de degré d

Le contexte d'application est l'approximation d'une fonction par un polynôme de base degré, notamment des fonctions utilisées en cryptographie. On peut aussi utiliser ces testeurs pour distinguer une fonction de chiffrement d'une fonction aléatoire.

6.6.4. Cryptanalyse des chiffrements à flot

Les systèmes de chiffrement à flot sont des algorithmes à clef secrète qui permettent de chiffrer et de déchiffrer à la volée, c'est-à-dire que tout bit de message peut être chiffré ou déchiffré sans qu'il soit nécessaire d'attendre la transmission des bits suivants. Ces algorithmes, qui ont également l'avantage d'être extrêmement rapides, sont donc très utilisés dans les applications embarquées, par exemple en téléphonie mobile. La plupart de ces systèmes utilisent des générateurs pseudo-aléatoires composés de registres à décalage à rétroaction linéaire. Dès lors que la sortie du générateur présente une corrélation avec la suite produite par l'un des registres employés, elle peut être assimilée au résultat de la transmission de cette suite à travers un canal bruité. La suite générée par un seul registre étant fortement redondante, on peut la reconstituer à l'aide d'un algorithme de décodage. L'efficacité de cette attaque, appelée attaque par corrélation rapide, dépend donc des performances du code correcteur utilisé pour représenter le système.

Anne Canteaut et Éric Filiol ont récemment amélioré les techniques classiques d'attaque par corrélation rapide dans le contexte des registres filtrés, c'est-à-dire des générateurs pseudo-aléatoires dont la sortie est obtenue en appliquant une fonction booléenne à certaines cellules d'un registre à décalage à rétroaction linéaire. Dans ce contexte particulier, il est en effet possible de tirer partie de tous les coefficients de Fourier non nuls de la fonction de filtrage. Cette attaque est actuellement la cryptanalyse la plus efficace sur les registres filtrés [51]. Une analyse précise a également permis de montrer que les performances de cette nouvelle attaque étaient pratiquement indépendantes des propriétés de la fonction de filtrage utilisée.

Une autre grande classe de générateurs pseudo-aléatoires utilisant des registres à décalage à rétroaction linéaire est celle des systèmes par combinaison. Les attaques par corrélation ont ici pour but de retrouver l'initialisation d'un petit ensemble de registres (c'est-à-dire une partie de la clef secrète) indépendamment des autres. Le nombre minimal de registres à attaquer simultanément est déterminé par l'ordre de corrélation de la fonction booléenne de combinaison. Mais les performances de l'attaque dépendent à la fois du nombre de registres attaqués, et de la qualité de l'approximation de la fonction de combinaison par une fonction qui ne dépend que de ces registres. Ainsi, si on augmente le nombre de registres considérés, on augmente la dimension du code à décoder, mais on diminue la probabilité d'erreur. Il est donc indispensable de déterminer le meilleur compromis entre ces deux paramètres. Dans ce but, Anne Canteaut s'est intéressée à la précision des approximations d'une fonction booléenne par des fonctions possédant moins de variables. Elle a notamment montré que toute fonction booléenne de haute non-linéarité (c'est-à-dire dont la distance aux fonctions affines est élevée) est nécessairement loin des fonctions possédant un petit nombre de variables. Ce résultat implique que le nombre optimal de registres mis en jeu dans les attaques par corrélation correspond exactement à l'ordre de corrélation de la fonction de combinaison [48].

6.7. Génération logicielle de nombres aléatoires

Participants : Nicolas Sendrier, André Seznec.

La question de la génération d'aléa a été très largement abordée et a conduit à deux grandes catégories de générateurs : les générateurs physiques et les générateurs pseudo-aléatoires. Les générateurs physiques consistent à faire des mesures sur des sources physiques d'aléa tels le bruit thermique des résistances électriques ou la décroissance exponentielle d'une population d'isotopes radioactifs. Les générateurs pseudo-aléatoires consistent, à partir d'une fonction bien choisie, à construire une suite récurrente chaotique pour une condition initiale donnée (appelée la « graine »).

En cryptographie, cette question de la production d'aléa est cruciale, en particulier pour générer les clefs de tous les algorithmes. Un biais statistique du générateur remet en cause la fiabilité de l'ensemble de l'algorithme de chiffrement. Cependant, les solutions que nous venons d'évoquer ne sont pas toujours satisfaisantes. Étant donnée l'ampleur de la population susceptible d'utiliser quotidiennement des applications cryptographiques, il semble nettement plus léger d'implémenter une solution logicielle pour générer de l'aléa et donc de renoncer aux générateurs physiques. Quant aux générateurs pseudo-aléatoires ils doivent malgré tout être initialisés par une graine réellement aléatoire.

Des solutions proposées et mises en oeuvre, par exemple pour le générateur d'aléa de Linux (/dev/random), exploitent les dates de divers événements ayant lieu sur une machine : clavier, souris, accès réseau... Ces événements ont en effet lieu à des dates qui ne sont pas toutes prévisibles à une fraction de seconde près et qui sont accessibles directement au niveau logiciel. Cependant, ces méthodes fournissent actuellement des débits extrêmement faibles, de l'ordre de l'octet par seconde dans le pire des cas. De tels débits peuvent se révéler problématiques dans certaines applications !

La grande complexité des processeurs modernes induit des variations du temps de calcul qui peuvent être importantes et qui sont liées à l'état interne de ce processeur (caches, pipe-line, prédicteur de branchement, ...). La possibilité, grâce au compteur de cycles disponible sur la plupart des architectures, de mesurer très précisément les temps d'exécution permet d'exploiter ces variations pour générer des nombres aléatoires. Des études préliminaires très prometteuses semblent indiquer que ce procédé est extrêmement performant. Une telle technique, si elle peut être validée à la fois théoriquement et pratiquement, autoriserait des débits d'aléa de qualité cryptographique qui n'étaient envisageables jusqu'alors que par des générateurs pseudo-aléatoire, ou par des procédé physiques externes à la machine. Ce travail a été initié lors d'un stage de Matthieu LEMOINE (ENSAE) de janvier à avril 2000. Le travail se poursuit en collaboration avec André Seznec (projet Caps, Irisa) dans le cadre de l'ARC Hipsor. Un produit logiciel est en cours d'élaboration.

6.8. Protection des droits d'auteurs - watermarking

Participants : Caroline Fontaine, Françoise Levy-dit-Vehel, Nicolas Sendrier.

Suite aux travaux sur le projet européen AQUARELLE, le thème du marquage d'images est resté dans le projet. Les participants sont C. Fontaine (LIFL), F. Levy-dit-Vehel (ENSTA), E. Lutton et F. Raynal (FRACTALES) et N. Sendrier (CODES). Notre intention est de maintenir pluri-compétences et synergies avec les applications (voir le projet iFIC dan la section suivante) sur un sujet où elles sont essentielles.

C. Fontaine a initié, dans le groupe de travail, l'élaboration d'un procédé de test des algorithmes de tatouage et la mise en place d'un serveur permettant à tout concepteur de mettre à l'épreuve son système. Un tel outil d'évaluation est nécessaire, car pour l'instant les algorithmes sont testés séparément, et suivant des critères différents, ce qui rend toute comparaison hasardeuse. Il faut également être très prudent sur la méthodologie à suivre, afin d'acquérir et de conserver la confiance des concepteurs envers nos tests. Ce projet a démarré il y a quelques mois et s'étend depuis à d'autres équipes, en France et à l'étranger.

C. Fontaine et F. Raynal (INRIA) travaillent egalement sur les liens précis qui existent entre la cryptographie et le tatouage des documents numériques. Ils s'intéressent à la transposition de concepts cryptographiques, tels les *protocoles zero-knowledge* (comment prouver à quelqu'un que l'on connait un secret, sans révéler aucune information sur celui-ci), le *partage de secret* (un secret est dispersé à travers n parts, et il en faut au moins k pour le reconstituer), ... dans le contexte du tatouage. Très peu de personnes se sont penchées sur cette approche car les communautés « cryptographie » et « traitement du signal » contiennent très peu de personnes en commun. Il nous parait important de faire le point sur les idées fausses et les liens réels qui existent dans ce domaine.

Un article a été presenté à la conference Electronic Imaging [70] en janvier 2002.

Françoise Levy-dit-Vehel participe au projet RNRT DIPHONET (DIffusion de PHOtographies à travers (I)nterNET - projet précompétitif, labellisé[5] en Mai 2001). Ce projet, mené en collaboration avec CANON Research France, l'IRISA (TEMICS, VISTA), SUPELEC (Laboratoire de Signaux et Systèmes) et ANDIA presse, se situe dans le contexte de la distribution de photographies numériques vers les professionnels et le grand public sur Internet. Le problème principal lié à la mise à disposition de photos au travers de réseaux ouverts est le pillage illicite de celles-ci. Ce problème, exprimé dans un contexte informatique, demande de mettre en place un environnement permettant d'une part de détecter qu'une image fait illégalement partie d'une collection d'images mises à disposition par un tiers (traçage de copies) et d'autre part d'exhiber une preuve de propriété irréfutable. Pour faciliter le traçage de copies illicites, nous proposons de combiner les techniques de tatouage et d'indexation par le contenu. Les preuves de propriété seront abordées au travers de l'utilisation conjointe de techniques de tatouage et de protocoles cryptographiques. Le résultat escompté du projet est une plate-forme logicielle de démonstration de la combinaison de ces techniques dans un système global adapté aux transactions sur Internet.

Tous les participants mentionnés plus haut interviendront pour définir l'architecture du système. Plus spécifiquement, la collaboration entre les équipes TEMICS et CODES s'articule selon deux directions :

- Tatouage robuste, multi-niveaux, et asymétrique : il s'agit ici d'une part d'élaborer un système de tatouage dont au moins une partie offre une grande résistance à des dégradations importantes de l'image (par exemple celles dues à la création d'une imagette). Dans notre contexte, ceci permettra un premier niveau de vérification de présence d'une marque par des techniques « légères ». Dans un deuxième temps, on souhaiterait avoir un tatouage tel que la détection de la présence d'une marque soit possible sans faire appel à la clef secrète de marquage (autrement dit, sans rendre la marque immédiatement obsolète). Cette fonctionnalité est, dans le principe, à rapprocher des techniques de cryptographie asymétrique. C'est d'ailleurs une approche de ce type que nous envisageons. Un prolongement fondamental de ce procédé serait ensuite l'extraction directe d'un certain type de marque à partir de seules données publiques (à savoir l'image marquée éventuellement altérée, et une clef publique de vérification).

[5] http://www.telecom.gouv.fr/rnrt/index_net.htm

- Preuve d'appartenance : l'étape ultime d'un processus de protection de propriété intellectuelle est celle - une fois le traçage de l'image réalisé - de la preuve d'appartenance. Celle-ci passe par la définition de protocoles cryptographiques dans ce contexte, c'est-à-dire en lien avec les algorithmes de tatouage utilisés pour le traçage.

6.9. Informatique quantique

Participants : Harold Ollivier, Jean-Pierre Tillich.

L'intérêt croissant pour l'informatique quantique, notamment dans la communauté des physiciens, a suscité de plus en plus de curiosité de la part des théoriciens de l'information dite classique, par opposition à quantique. Plusieurs domaines ont été abordés au sein du projet CODES au cours de l'année précédente.

Les ordinateurs quantiques potentiels seront, et les premiers prototypes le montrent amplement, particulièrement sujets à la décohérence. Ce phénomène de perte des propriétés quantiques est dû à la corrélation des registres de calcul avec leur environnement. Ainsi, il est possible de caractériser certains aspects de la décohérence grâce à la théorie de l'information. Nous avons apporté notre contribution à cette recherche en établissant une collaboration avec Los Alamos National Laboratory.

De plus cette interaction a mis en évidence l'intérêt intrinsèque des quantités issues de la théorie de l'information pour l'étude de paradoxes purement quantiques dans le cadre de problèmes de communication, tel la non-localité sans enchevêtrement.

Face à la décohérence, il est heureusement possible d'envisager des stratégies de préservation de l'information : les codes correcteurs et les sous-systèmes sans décohérence. C'est à la première que nous sommes plus particulièrement intéresses. Nous espérons pouvoir améliorer les capacités de correction ainsi que notre compréhension des mécanismes de correction d'erreurs quantiques. Sur ces différents problèmes, nous collaborons avec le Laboratoire de Recherche en Informatique de l'Université Paris Sud.

Enfin, à l'initiative d'un groupe de travail informel réunissant de jeunes chercheurs (LKB-ENS, LRI-Orsay, CODES-INRIA), nous avons commencé à proposer des séquences expérimentales pour des prototypes de processeurs quantiques existants, ou prochainement disponibles, afin de réaliser des versions simples d'algorithmes quantiques (clonage imparfait, porte élémentaire de Toffoli). Cette collaboration s'est considérablement renforcée avec le Laboratoire Kasler-Brossel de l'Ecole Normale Supérieure.

7. Contrats industriels

Nous décrivons dans ce paragraphe nos activités de transfert scientifique et développement.

7.1.1. Collaboration CNET/INRIA+LACO :

Étude de nouveaux turbo-codes en bloc, les codes CORTEX, 99-2001, demandé à être prolongé en 2002. Un contrat a été signé fin 1999 entre le CNET (CCETT, Rennes) et l'INRIA (projet CODES). Coté INRIA, il s'agit d'une collaboration entre les chercheurs de CODES, ceux du Laboratoire d'Arithmétique, Codage et Optimisation de l'Université de Limoges et J.-P. Tillich du LRI d'Orsay. Les responsables sont : T. Berger (LACO), P. Charpin (INRIA et LRI) et J.-C. Carlach (CNET).

Le travail proposé consiste en l'étude d'une nouvelle famille de codes en blocs, que nous avons nommés *codes Cortex*. L'étude théorique a pour but d'analyser les bornes de performance de ces nouveaux codes. L'étude pratique consiste principalement à écrire des logiciels réalisant des codeurs et des décodeurs de ces codes, permettant ainsi de valider les niveaux de performance indiqués par l'étude théorique.

Cette étude s'insère dans *la recherche de codes correcteurs d'erreurs pour les futurs systèmes de transmissions hertziennes*. Dans ces futurs systèmes les informations sont transmises par petits paquets ou blocs de données. La longueur de ces paquets est limitée à quelques centaines de bits, ce qui impose l'utilisation de codes correcteurs d'erreurs courts les meilleurs possibles afin de maximiser le nombre de bits utiles par paquet pour une capacité de correction d'erreurs donnée. L'algorithmique sous-jacente est ici fondamentale et l'on s'intéresse, en particulier, aux techniques les plus récentes du *décodage itératif* (voir § 6.3).

Le contrat sur les codes CORTEX constitue un véritable transfert scientifique. En outre, il implique une collaboration suivie entre le CCETT et une communauté fournie de chercheurs et doctorants, sur les aspects théoriques et appliqués de l'étude menée ainsi que sur ses perspectives.

Ce contrat est prolongé en Septembre 2002 sous le titre « Recherche d'alternative aux turbos-codes ».

7.1.2. CrAC I et CrAC II

- Action Concertée Incitative « Cryptologie » (août 2002 - août 2005)
Titre : *CrAC II - Cryptologie, Algorithmique et Codes II*
Coordinatrice du projet : A. Canteaut.
Intervenants : C. Carlet, P. Charpin, M. Finiasz, F. Galand, N. Sendrier, C. Tavernier, M. Videau
Le projet CRAC II s'inscrit dans le prolongement du projet CRAC présenté par les chercheurs du projet CODES et soutenu par l'ACI Cryptologie 2000 (soutien aux équipes d'excellence, 600 kF sur 3 ans). Son objectif est d'approfondir les travaux de l'équipe sur les systèmes à clef publique fondés sur les codes et sur la cryptographie symétrique, qui font l'objet de plusieurs thèses de doctorat débutées récemment au sein de CODES. Il a également pour but de renforcer les collaborations scientifiques initiées par le projet CRAC. Ce projet a obtenu un financement du Ministère de la Recherche de 75 000 Euros sur une durée de trois ans à partir d'août 2002.

7.1.3. ACI PolyCrypt

Cette Action Concertée incitative se situe dans le cadre des échanges entre calcul formel et cryptologie. Elle est encadrée par Guillaume Hanrot, et les équipes Codes, Spaces (Loria et Rocquencourt) y participent. Un premier succés a été obtenu par Jean-Charles Faugère de Spaces, qui a réussi a « casser » le premier challenge HFE. Tous les aspects algébriques de la cryptanalyse sont abordés dans cette ACI, notamment les attaques par bases de Gröebner.

7.1.4. ACI ACCESS

Outils algébriques et combinatoires pour la construction et l'étude de systèmes à clé publique. Ctte ACI obtenue par Françoise Levy-dit-Vehel et Pierre Loidreau est gérée par le projet Codes, qui y est ainsi impliqué.

8. Actions régionales, nationales et internationales

8.1. Actions nationales

Collaboration scientifique et échanges se sont poursuivis en 2002, 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, Lille et avec l'ENSTA 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 et les écoles.

Notre collaboration scientifique, avec nos chercheurs extérieurs, a aussi pour objectif d'accroître notre domaine de compétences en mathématiques. Ceci se concrétise par des travaux en commun ou des co-directions de thèses.

8.1.1. Contrats nationaux

- Action Concertée Incitative « Cryptologie », premier appel. Un premier rapport d'évaluation a été rendu en 2002.

- Action Concertée Incitative « Cryptologie », deuxième appel. Notre projet, soumis au deuxième appel d'offre a été retenu dans le cadre du *soutien aux équipes d'excellence* pour un financement de trois ans à partir d'Août 2002.
Titre : *Cryptologie, Algorithmique et Codes* ;
Coordinateur du projet : Anne Canteaut ;

Intervenants : Daniel Augot, Anne Canteaut, Nicolas Sendrier (projet CODES) et Claude Carlet (Paris 8 et CODES).
Le programme scientifique est fondé sur les compétences des intervenants sur les problèmes mathématiques et algorithmiques liés à la protection de l'information. Dans chacun des domaines de recherche, cryptographie symétrique, cryptographie asymétrique et cryptanalyse, nous proposons des thèmes prioritaires. L'objectif est d'approfondir les travaux de l'équipe sur les systèmes à clef publique fondés sur les codes et sur la cryptographie symétrique, qui font l'objet de plusieurs thèses de doctorat débutées récemment au sein de CODES. Il a également pour but de renforcer les collaborations scientifiques initiées par le projet CRAC.

Enfin notre proposition s'inscrit dans un ensemble de synergies avec des interfaces et liens thématiques au plan national et le renforcement de nos collaborations internationales sur nos thèmes de recherche.
- Action Concertée Incitative « Cryptologie », deuxième appel.
Titre : *Calcul formel en cryptologie : algorithmes, interactions et applications* ;
Coordinateur du projet : Guillaume Hanrot (projet SPACES) ;
Intervenants : Daniel Augot, Cédric Tavernier.
Il s'agit d'une action d'interface, qui regroupe les projet CODES et SPACES, sur trois sites : Rocquencourt, Paris VI (Bâtiment Scott), et Nancy. Trois axes sont dégagés :

- cryptanalyse de HFE : c'est un horizon qui motive les autres développements ;
- calcul de bases de Groebner sur les corps finis ;
- développement d'une librairie efficace de calcul dans les corps finis.

8.1.2. Groupes de recherche

Le projet participe à :

- GDR *Algorithmes Langages et Programmation* (AMI) : Claude Carlet a la responsabilité du groupe de travail intitulé *Codage et Cryptographie*. Il a organisé les journées du groupe de travail C2 du GDR ALP 12 au 15 novembre 2002, au CIRM (avec Pierre Liardet et Robert Rolland).
- au GdR Information quantique (Harold Ollivier).

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.

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[6] depuis octobre 99.

D. Augot et Cédric Tavernier sont chargés de l'organisation du séminaire du projet CODES.

[6] http://www.ensta.fr/~loidreau/CCA/cca.html

8.1.3. Participations à des instances et manifestations nationales

Plusieurs membres du projet participent à des commissions de spécialistes :

Université de Paris 8, 25e section (cnu) : C. Carlet.

Université de Limoges, 25e section (cnu) : T. Berger, A. Canteaut, C. Carlet, P. Charpin, F. Laubie, P. Gaborit.

Université du Var, 27e section (cnu) : C. Carlet, P. Charpin.

INRIA-Rocquencourt, section d'audition du jury CR2 2001 : P. Charpin.

J.P. Tillich est membre de la commission de spécialistes de l'Ecole Normale Supérieure (27e section.

T. Berger est membre de la commission de spécialiste 25-26-27-72èmes section de Paris VIII.

Claude Carlet est élu au Conseil Scientifique de l'Université Paris 8, président de l'une des 4 commissions d'évaluation de l'Université Paris 8 (qui expertisent les demandes d'habilitations d'équipes de recherche).

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

P. Charpin est membre membre du conseil de l'école doctorale de l'Université de Limoges.

P. Charpin est membre du comité scientifique de l'Action Concertée Incitative (ACI) « Cryptologie », ministère de la recherche.

P. Charpin est responsable de l'ACI CRAC *Cryptologie, Algorithmique et Codes*, (2000-2003).

A. Canteaut est responsable de l'ACI CRAC-II.

C .Fontaine est le correspondant local (au LIFL) du GDR ISIS (Information, Signal, Images et viSion) ainsi que du groupe C2 (Codage et Cryptographie) du GDR ALP (Algorithme, Langage et Programmation).

8.2. Actions internationales

8.2.1. 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 Computers*, *Designs Codes and Cryptography*, *Discrete Mathematics*, *Journal of Cryptology*, *Finite Fields*, les conférences *EUROCRYPT*, *Fast Software Encryption (FSE)* et *IEEE symposium on Information Theory* (ISIT).

Organisation de rencontres internationales :

- A. Canteaut est membre du comité de programme de la conférence *YACC 2002*, Porquerolles, France, juin 2002.
- A. Canteaut est membre du comité de programme de FSE 2002 (Fast Software Encryption), Lund (Suède), 24-26 février 2003.
- A. Canteaut et N. Sendrier sont membres du comité de programme du IEEE Information Theory Workshop, Paris, 31 mars - 4 avril 2003.
- Les membres du projet préparent le colloque international WCC »03 *Workshop on Coding and Cryptography 2003*, 24-28 mars 2003, Versailles, France. Le comité de programme est présidé par P. Charpin (co-présidence avec G. Kabatianski) et le comité d'organisation par P. Loidreau. Il y a eu 107 soumissions.
  (cf. http://www-rocq.inria.fr/codes/WCC2003).
- C. Carlet est membre du comité de programme de CCC (International Workshop on Coding, Cryptography, and Combinatorics), 23-28 Juin 2003, Yellow Mountains, (comité de programme co-dirigé par Harald Niederreiter).
- C. Carlet est membre du comité de programme d'AAECC 15, Mai 2003, Toulouse (comité de programme dirigé par A. Poli). item C. Carlet est membre du comité de programme de Fq7 (Finite Fields and Applications), Mai 2003 Toulouse (comité de programme dirigé par A. Poli).

Revues :

- C. Carlet est Associate Editor pour la revue « IEEE Transactions on Information Theory » (spécialité « Coding Theory »).
- P. Charpin est membre du comité d'édition de la revue internationale *Designs, Codes and Cryptography*.
- P. Charpin est membre du conseil consultatif de l'encyclopédie de cryptologie intitulée *Encyclopedia of Information Security*.
- Éditrice associée : Pascale Charpin pour *IEEE Transactions on Computers*, dans la spécialité *codage*.
- Special issue in Coding and Cryptography, Éditeur : Claude Carlet, à paraître dans la revue Discrete Applied Mathematics.
- N. Sendrier est membre du comité de lecture d'un numéro de TSI sur le thème « Sécurité informatique » (septembre 2002).

8.2.2. Accueils de chercheurs étrangers

Le projet a une politique d'invitation « large », au plan national et au plan international. Le projet a accueilli, pour de courtes durées, en 2002 :

- Hans Dobbertin, Magnus Daum, Patrick Felke, Tanja Lange, Gregor Leander (University of Bochum, Allemagne) ;
- Joel Friedman (University of British Columbia, Vancouver, Canada) ;
- Gregory Kabatianski (IPIT, Moscou, Russie) ;
- James L. Massey (Lund University, Suède) ;
- Gary McGuire (National University of Ireland) ;
- Alexei V. Ourivski (Institut de Physique et de Technologies, Moscou, Russie) ;
- Henk van Tilborg (Eindhoven University, Pays-Bas) ;
- Alexander Vardy (Université de Californie, San Diego, USA).

9. Diffusion des résultats

9.1. 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 le DEA parisien :

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 :

- T. Berger est responsable de la formation doctorale de mathématiques de l'Université de Limoges.
- T. Berger est membre du bureau de l'école doctorale Science, Technologie, Santé de Limoges.
- Daniel Augot et Jean-Pierre Tillich interviennent dans le DEA Algorithmique, filière Traitement et protection de l'Information, pour assurer un cours de codes correcteurs d'erreurs.
- J.P. Tillich intervient dans le DESS d'ingéniérie Mathématique de l'Université de Paris-Sud.
- J.P. Tillich est responsable du cours « Algoritmique, programmation et complexité » en licence d'informatique à l'Université de Paris-Sud.
- A. Canteaut enseigne la *programmation en langage* C dans le DEA *Cryptographie, Codage, Calcul* et dans le DESS *Sécurité de l'information* de l'Université de Limoges. Ce cours met en particulier l'accent sur les techniques algorithmiques spécifiques à la cryptographie et au codage.

- N. Sendrier est chargé d'enseignement à l'École Polytechnique au département d'informatique. Cours enseignés : Algorithmique et programmation (travaux dirigés), Introduction à la théorie de l'information (cours + TD).
- TPs de cryptographie, P. Loidreau à l'ENSTA.
- F. Levy-dit-Vehel enseigne un cours « Primitives cryptographiques » en troisième année à l'ENSTA.
- N. Sendrier est chargé de TP à l'École polytechnique, (tronc commun Informatique) depuis octobre 00.

Les chercheurs du projet participent par ailleurs à diverses actions de formation. Par exemple,

- N. Sendrier est organisateur de la session cryptographie aux « Journées Nationales de Calcul Formel 2003 », Luminy, janvier 2003.
- P. Gaborit est organisateur depuis 3 ans des journées annuelles de Cryptographie de Limoges

9.2. Jurys de thèse

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

Janvier 02 C. VERVOUX,
Contribution vers l'accélération de l'algorithme de Buchberger en combinant la méthode de coupure de Knuth-Schönhage et une approche de type sous-résultants,
Université de Limoges.
Jury : T. Berger (examinateur)

Février 02 A. LOBSTEIN,
Contribution combinatoire au codage, en connexion avec la complexité et la cryptographie,
Habilitation à diriger des Recherches, Université Paris 6.
Jury : P. Charpin (rapporteur).

Mars 02 N. SENDRIER,
Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs,
Mémoire d'habilitation, Université Paris 6.
Jury : P. Charpin, T. Berger (examinateurs).

Mars 02 FRÉDÉRIC RAYNAL,
Etude d'outils pour la dissimulation d'information : approches fractales, protocoles d'évaluation et protocoles cryptographiques, université Paris XI.
Jury : F. Levy-dit-Vehel (examinateur).

Juin 02 J. BYUN,
Système d'hordatage dans un environnement de réseau ouvert, université de Toulon et du Var.
Jury : C. Fontaine (examinateur).

Septembre 02 M. MINIER,
Preuves d'analyse et de sécurité en cryptologie à clé secrète,
Université de Limoges.
Jury : P. Charpin (rapporteur), T. Berger, A. Canteaut (examinateurs).

Novembre 02 G. ZÉMOR,
Contribution à la combinatoire et aux codes correcteurs,
Habilitation à diriger des Recherches, Université Paris 7.
Jury : P. Charpin (rapporteur).

Novembre 02 D. MASSON,
Université de Bordeaux.
Jury : P. Gaborit (examinateur).

Décembre 02 A. OTMANI,
Codes CORTEX *et constructions de codes autoduaux optimaux*,
Thèse de l'Université de Limoges.
P. Charpin, P. Gaborit, J-P. Tillich (membres du jury).

9.3. 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 ou laboratoires en 2002 :

- Collaboration avec Los Alamos National Laboratory et l'université de Californie. Harold Ollivier a été invité de février à juin, de août à septembre. Et aussi, avec Perimeter Institute Canada de novembre à décembre.
- Collaboration avec l'univeristé de Mexcico. Claude Carlet a été invité en juillet pendant une semaine.
- Invitation de Marion Videau par le Professeur Hyun Kwang Kim au Combinatorial and Computational Mathematics Center (Com2MaC) du 15 juillet au 18 août, Pohang, Corée du Sud.

Participations aux colloques en 2002 :

- PKC *Public Key Cryptography*, Paris, France, 12-14 février 2002.
  Participant : M. Finiasz.
- FSE, Leuven, Belgique, 4-6 février 2002.
  Participants : D. Augot, A. Canteaut, C. Tavernier.
- EUROCRYPT'02, Amsterdam, Pays-Bas, 28 avril - 2 mai 2002.
  Conférencières : A. Canteaut, M. Videau.
  Participants : C. Carlet, P. Charpin, M. Finiasz, F. Lévy-dit-Véhel, N. Sendrier.
- *Workshop in honor of Bob McEliece's 60th birthday*, Caltech, Pasadena, USA, 24-25 mai 2002.
  Conférenciers invités : A. Canteaut, N. Sendrier.
- *Symposium on Information Theory in the Benelux*, Louvain-la-Neuve, Belgique, 29-31 mai 2002.
  Conférenciers : C. Carlet, É. Filiol.
- YACC'02, Iles de Porquerolles, France, 3-7 juin 2002.
  Conférencière invitée : A. Canteaut.
  Participant : C. Carlet.
- ISIT'02 - *IEEE International Symposium on Information Theory*, Lausanne, Suisse, 30 juin - 5 juillet 2002.
  Conférenciers : D. Augot, T. Berger, A. Canteaut, P. Charpin, M. Finiasz, P. Gaborit, P. Loidreau, N. Sendrier, J.-P. Tillich, M. Videau.
- *Coloquio Nacional de Teoria de Codigos, Criptografia*, Mexico, Mexique, 17-19 juillet 2002.
  Conférencier invité : C. Carlet.
- SIAM *Conference on Discrete Mathematics*, San Diego, USA, 11-14 août 2002.
  Conférencier : C. Carlet.
- *Crypto*, Santa Barbara, USA, 18-22 août 2002.
  Conférencier : C. Carlet.
- ACCT-8 - *8th International Workshop on Algebraic and Combinatorial Coding Theory*, St Petersbourg, Russie, 8-14 septembre 2002.
  Conférenciers : T. Berger, G. Olocco, C. Tavernier.
  Participants : P. Charpin, P. Loidreau, N. Sendrier.
- *Rencontre Arithmétique et Combinatoire*, CIRM-Luminy, France, 23-27 septembre 2002.
  Participant : C. Carlet.

- ITW'02 - *IEEE Information Theory Workshop*, Bangalore, Inde, 20-25 octobre 2002.
  Conférencière invitée : A. Canteaut.
- *5th International Workshop on Information Hiding*, Noordwijkerhout, Pays-Bas, 7-9 octobre 2002.
  Participants : C. Fontaine, F. Galand.
- *Journée C2 (Codes et Cryptographie)*, CIRM-Luminy, France, 12-15 novembre 2002.
  Organisateur : C. Carlet.
  Conférenciers : T. Berger, C. Carlet, É. Filiol, C. Fontaine, F. Galand, P. Loidreau, C. Nedeloaia, L. Perret.
- STORK - *Cryptography Workshop*, Bruges, Belgique, 26-27 novembre 2002.
  Participants : D. Augot, A. Canteaut, N. Sendrier.
- *Asiacrypt'02*, Queenstown, Nouvelle-Zélande, 1-5 décembre 2002.
  Conférencier : C. Carlet.
- *1st Workshop on Security in Ad-Hoc Networks*, Ruhr University Bochum, Allemagne, 2 décembre 2002.
  Participant : R. Bhaskar.
- ICICS'02 - *4th International Conference on Information and Communication Security*, Singapour, 9-12 décembre 2002.
  Conférencier : É. Filiol.

10. Bibliographie

Bibliographie de référence

[1] D. AUGOT. *Description of minimum weight codewords of cyclic codes by algebraic systems.* in « Finite Fields and their Applications », numéro 2, 1996, pages 138-152.

[2] D. AUGOT, J.-M. BOUCQUEAU, J.-F. DELAIGLE, C. FONTAINE, E. GORAY. *Secure delivery of images over open networks.* in « Proceedings of the IEEE », numéro 7, volume 87, juillet, 1999, pages 1251-1266, (Special Issue on « Identification and protection of multimedia information »), article invité.

[3] T. BERGER, P. CHARPIN. *The permutation group of affine-invariant extended cyclic codes.* in « IEEE Transaction on Information Theory », numéro 6, volume 42, novembre, 1996, pages 2194-2209.

[4] 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.* in « IEEE Transactions on Information Theory », numéro 1, volume 44, janvier, 1998, pages 367-378.

[5] A. CANTEAUT, P. CHARPIN, H. DOBBERTIN. *Binary m-sequences with three-valued crosscorrelation : A proof of Welch conjecture.* in « IEEE Transactions on Information Theory », numéro 1, volume 46, 2000, pages 4-8.

[6] A. CANTEAUT, P. CHARPIN, H. DOBBERTIN. *Weight divisibility of cyclic codes, highly nonlinear functions on GF(2^m) and crosscorrelation of maximum-length sequences.* in « SIAM Journal on Discrete Mathematics », numéro 1, volume 13, 2000, pages 105-138.

[7] C. CARLET, P. CHARPIN, V. ZINOVIEV. *Codes, bent functions and permutations suitable for DES-like cryptosystems.* in « Designs Codes and Cryptography », numéro 15, 1998, pages 125-156.

[8] C. CARLET, P. GUILLOT. *A characterization of binary bent functions.* in « Journal of Combinatorial Theory, Series A », numéro 2, volume 76, 1996, pages 328-335.

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

[10] É. FILIOL, C. FONTAINE. *Highly nonlinear balanced Boolean functions with a good correlation-immunity.* in « Advances in Cryptology - EUROCRYPT'98 », série Lecture Notes in Computer Science, numéro 1403, Springer Verlag, pages 475-488, 1998.

[11] G. HACHÉ, D. LE BRIGAND. *Effective construction of algebraic geometry codes.* in « IEEE Transaction on Information Theory », numéro Numéro spécial : Algebraic Geometry Codes, 6, volume 41, 1996, pages 1615-1628.

[12] N. SENDRIER. *On the dimension of the hull.* in « SIAM Journal on Applied Mathematics », numéro 2, volume 10, mai, 1997, pages 282-293.

Thèses et habilitations à diriger des recherche

[13] N. SENDRIER. *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs.* Mémoire d'habilitation à diriger des recherches, Université Paris 6, 2002, http://www-rocq.inria.fr/codes/Nicolas.Sendrier/.

Articles et chapitres de livre

[14] C. BACHOC, P. GABORIT. *Designs and self-dual codes with long shadows.* in « Journal of Comb. Theory Series A », 2002, submitted.

[15] T. BERGER. *Automorphism Groups of Homogeneous and Projective Reed-Muller Codes.*. 2002.

[16] T. BERGER, P. LOIDREAU. *How to mask the structure of codes for a cryptographic use.* soumis.

[17] A. CANTEAUT. *Cryptanalyse de chiffrement à clef secrète par blocs.* in « MISC - Le magazine de la sécurité informatique », numéro 2, mars, 2002.

[18] A. CANTEAUT. *Le chiffrement à la volée.* in « Pour la Science », juillet, 2002, pages 86-87, Numéro spécial *La cryptographie, l'art du secret*.

[19] C. CARLET. *On the divisibility properties and nonlinearity of resilient functions.* in « Comptes Rendus de l'Académie des Sciences de Paris », numéro t. 331, Serie 1, 2000, pages 917-922.

[20] C. CARLET, P. SARKAR. *Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions.* in « Finite fields and Applications », volume 8, 2002, pages 120-130.

[21] C. CARLET, Y. TARANNIKOV. *Covering sequences of Boolean functions and their cryptographic significance.* in « Designs, Codes and Cryptography », volume 25, 2002, pages 263-279.

[22] P. CHARPIN, E. PASALIC. *On propagation characteristics of resilient functions.* in « Selected Areas in Cryptography, SAC 2002 », 2002, LNCS, Springer-Verlag, à paraître.

[23] A. N. F. ARNAULT. *Feedback with Carry Shift Registers synthesis with the Euclidean Algorithm.* soumis.

[24] E. FILIOL. *Analyse du virus CONCEPT.* in « MISC », numéro 4, 2002.

[25] E. FILIOL. *L'ingéniérie sociale.* in « Linux Magazine France », numéro 42, 2002.

[26] E. FILIOL. *Le ver Codered.* in « MISC », numéro 2, 2002.

[27] E. FILIOL. *Le virus CIH dit "Chernobyl".* in « MISC », numéro 3, 2002.

[28] P. GABORIT. *Construction of new unimodular lattices.* in « European Jour. Combin. », 2002.

[29] P. GABORIT. *Quadratic Double Circulant Codes over Fields.* in « J. Comb. Theory (A) », numéro 97, 2002, pages 85-107.

[30] P. GABORIT, J. KIM, V. PLESS. *Decoding binary R(2,5) by hand.* in « Discrete Math », 2002, to appear.

[31] P. GABORIT, A. OTMANI. *Experimental construction of self-dual codes.* in « Finite Fields and their Applications », 2002, submitted.

[32] P. GABORIT, V. PLESS, P. SOLÉ, A. O. L. ATKIN. *On Type II Codes over GF(4).* in « Finite Fields and Appl. », numéro 8, 2002, pages 171-183.

[33] P. LOIDREAU. *L'identification a divulgation nulle de connaissance.* in « MISC », numéro 1, 2002.

[34] P. LOIDREAU. *Le partage de secret.* in « MISC », numéro 3, 2002.

[35] P. LOIDREAU. *Le transfert inconscient.* in « MISC », volume 2, 2002.

[36] P. MILMAN, H. OLLIVIER, J. M. RAIMOND. *Universal Quantum Cloning in Cavity QED.* LANL Preprint, quant-ph/0207039.

[37] C. NEDELOAIA. *Weight Distributions of Cyclic Self-Dual Codes.* in « IEEE Transactions on Information Theory », 2003, submitted.

[38] H. OLLIVIER, D. POULIN, W. H. ZUREK. *Emergence of objective properties from subjective quantum states : Environment as a witness.*

[39] H. OLLIVIER, W. H. ZUREK. *Quantum discord : A measure of the quantumness of correlations.* in « Phys. Rev. Lett. », volume 88, 2002, pages 17901, LANL Preprint, quant-ph/0105072.

[40] P. G. R. CHAPMAN, P. SOLÉ. *2-modular lattices from ternary codes.* in « J. Théorie des Nombres de Bordeaux », numéro 14, 2002, pages 73-85.

[41] N. SENDRIER. *On the security of the McEliece public-key cryptosystem.* éditeurs M. BLAUM, P. FARRELL, H. VAN TILBORG., in « Information, Coding and Mathematics », Kluwer, 2002, pages 141-163, Proceedings of Workshop honoring Prof. Bob McEliece on his 60th birthday.

Communications à des congrès, colloques, etc.

[42] D. AUGOT, M. FINIASZ. *A Public Key encryption scheme based on the Polynomial Reconstruction problem.* in « Eurocrypt 2003 », 2003, submitted.

[43] T. BERGER. *Isometries for rank distance and permutation group of Gabidulin codes.* in « Proceedings of ACCT'7, (septembre 2002 », pages 30-33, St Petersbourg, 2002.

[44] T. BERGER, P. LOIDREAU. *Security of the Niederreiter version of the GPT public key cryptosystem.* in « Proceedings of IEEE ISIT 2002 », pages 267, Lausanne, Suisse, 2002.

[45] T. P. BERGER, P. LOIDREAU. *Security of the Niederreiter form of the GPT public-key cryptosystem.* in « IEEE International Symposium on Information Theory, ISIT 2002 », 2002.

[46] A. CANTEAUT. *Cryptanalysis of Block Ciphers and Related Properties of the Walsh Spectra of S-boxes.* in « YACC 02 », pages 3-4, Porquerolles, France, june, 2002.

[47] A. CANTEAUT. *Design criteria for symmetric primitives.* in « STORK Cryptography Workshop - Position papers », pages 44-45, Bruges, Belgique, novembre, 2002.

[48] A. CANTEAUT. *On the correlations between a combining function and functions of fewer variables.* in « Proceedings of 2002 IEEE Information Theory Workshop », IEEE, pages 78-81, Bangalore, Inde, octobre, 2002.

[49] A. CANTEAUT, P. CHARPIN. *Decomposing bent functions.* in « Proceedings 2002 IEEE International Symposium on Information Theory », IEEE, pages 42, Lausanne, Suisse, juillet, 2002.

[50] A. CANTEAUT, P. CHARPIN, M. VIDEAU. *Cryptanalysis of Block Ciphers and Weight Divisibility of Some Binary Codes.* in « Information, Coding and Mathematics (Workshop honoring Bob McEliece on his 60th birthday) », Kluwer, éditeurs H. V. T. M. BLAUM., 2002, Article invité.

[51] A. CANTEAUT, E. FILIOL. *On the Influence of the Filtering Function on the Performance of Fast Correlation Attacks on Filter Generators.* in « Proceedings of 23rd Symposium on Information Theory in the Benelux », Louvain-la-Neuve, Belgique, mai, 2002.

[52] A. CANTEAUT, M. VIDEAU. *Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis.* in « Advances in Cryptology - EUROCRYPT 2002 », série Lecture Notes in Computer Science, numéro 2332, Springer-Verlag, pages 518-533, 2002.

[53] A. CANTEAUT, M. VIDEAU. *Higher order differential attacks on iterated block ciphers using almost bent round functions.* in « Proceedings 2002 IEEE International Symposium on Information Theory », IEEE, pages 209, Lausanne, Suisse, juillet, 2002.

[54] C. CARLET. *A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction.* in « CRYPT0 2002, Advances in Cryptology », série Lecture Notes in Computer Science, numéro 2442, Springer-Verlag, pages 549-564, 2002.

[55] C. CARLET. *On cryptographic complexity of Boolean functions.* in « Fq6 : Finite Fields and Applications », 2002.

[56] C. CARLET, A. KLAPPER. *Upper bounds on the numbers of resilient functions and of bent functions.* in « YACC 02 », série Porquerolles, France, June, 2002.

[57] P. CHARPIN, A. CANTEAUT, M. VIDEAU. *Cryptanalysis of block ciphers and weight divisibility of some binary codes.* in « Information, Coding and Mathematics (Workshop in honor of Bob McEliece's 60th birthday) », Kluwer, 2002, invited paper.

[58] P. CHARPIN, E. PASALIC. *On propagation characteristics of resilient functions.* in « Selected Areas in Cryptography, SAC 2002 », série LNCS, Springer-verlag, 2002.

[59] N. COURTOIS, M. FINIASZ, N. SENDRIER. *Short McEliece-based Digital Signatures.* in « Proceedings 2002 IEEE ISIT ».

[60] C. ET A. GOUGET. *An upper bound on the number of m-resilient Boolean functions.* in « ASIACRYPT 2002, Advances in Cryptology », série Lecture Notes in Computer Science, Springer-Verlag, 2002.

[61] C. C. ET A. KLAPPER. *Upper bounds on the numbers of resilient functions and of bent functions.* in « 23rd Symposium on Information Theory in the Benelux », 2002.

[62] A. N. F. ARNAULT. *A new class of stream ciphers combining LFSR and FCSR architectures.* in « Indocrypt'02, (décembre 2002 », Hyderabad, Inde, 2002, à paraître.

[63] A. N. F. ARNAULT. *Feedback with Carry Shift Registers synthesis with the Euclidean Algorithm.* in « Proceedings of IEEE ISIT 2002 », pages 69, Lausanne, Suisse, 2002.

[64] É. FILIOL. *Decimation attack of stream ciphers.* in « Proceedings of the First International Conference - INDOCRYPT'2000 », série Lecture Notes in Computer Science, volume 1977, Indian Statistical Institute, Springer Verlag, éditeurs E. O. BIMAL ROY., pages 31-42, India, Calcutta, December, 2000.

[65] E. FILIOL. *A New Statistical Testing for Symmetric Ciphers and Hash Functions.* in « 4th International Conference in Communications and Security », série Lecture Notes in Computer Science, Springer Verlag, 2002.

[66] C. FONTAINE, F. RAYNAL. *About the links between cryptography and information hiding.* in « IS&T/SPIE International Symposium on Electronic Imaging 2002 », série Proceedings of the SPIE, volume 4675, SPIE,

2002.

[67] P. GABORIT, A. OTMANI. *Experimental construction of self-dual codes over GF(3) and GF(4).* in « Int. Sympos. Inf. Theory (ISIT 2002 », pages 459, 2002.

[68] C. NEDELOAIA. *On Weight Distribution of Cyclic Self-Dual Codes.* in « International Symposium on Information Theory (ISIT 2002) », 2002.

[69] G. OLOCCO, A. OTMANI. *Low Complexity Tail-Biting Trellises for Some Extremal Self-Dual Codes.* in « Eight International Workshop On Algebraic and Combinatorial Coding Theory », 2002.

[70] F. RAYNAL, C. FONTAINE. *About the links between cryptography and data hiding.* in « IS&T/SPIE International Symposium on Electronic Imaging 2002 », série Proceedings of the SPIE, volume 4675, SPIE, 2002.

[71] N. SENDRIER, D. AUGOT, M. FINIASZ, P. LOIDREAU. *Diversity in public key cryptography using coding theory and related problems.* in « STORK cryptography workshop », Bruges, Belgium, novembre, 2002.

[72] N. SENDRIER. *A Practical Digital Signature Scheme Based on Coding Theory.* in « CAL-(IT)^2 Seminar », UCSD, San-Diego, CA, USA, mai, 2002.

[73] N. SENDRIER. *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs : état de l'art et problèmes ouverts.* in « Colloque de l'ACI cryptologie », La Bussière sur Ouche, France, Octobre, 2002.

[74] N. SENDRIER. *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs : état de l'art et problèmes ouverts.* in « Journée sécurité du LIX », École Polytechnique, Palaiseau, France, Septembre, 2002.

[75] N. SENDRIER. *On the security of the McEliece public-key cryptosystem.* in « Workshop honoring Prof. Bob McEliece on his 60th birthday », Caltech, Passadena, CA, USA, mai, 2002.

[76] J. TILLICH, G. ZÉMOR. *The gaussian isoperimetric inequality and the probability of a decoding error.* in « ISIT 2002 », 2002.

Rapports de recherche et publications internes

[77] A. CANTEAUT, M. VIDEAU. *Weakness of Block Ciphers Using Highly Nonlinear Confusion Functions.* Rapport de recherche, numéro RR-4367, INRIA, février, 2002, http://www.inria.fr/rrrt/rr-4367.html.

[78] P. CHARPIN, E. PASALIC. *Propriétés de propagation des fonctions résilientes.* rapport de recherche, numéro 4537, INRIA, Septembre, 2002, http://www.inria.fr/rrrt/rr-4537.html.

[79] F. L. DIT-VÉHEL, L. PERRET. *A Polly Cracker system based on satisfiability".* rapport technique, ENSTA, 2002, à paraître.

[80] E. FILIOL. *Applied Cryptanalysis and Computer Attack through Hidden Ciphertext Computer Viruses.* rapport technique, numéro RR-4359, INRIA, 2002, http://www.inria.fr/rrrt/rr-4359.html.

[81] P. GABORIT, J. OHLER, P. SOLÉ. *CTRU, a polynomial analogue of NTRU.* rapport technique, numéro RR-4621, INRIA, 2002, http://www.inria.fr/rrrt/rr-4621.html.

Divers

[82] P. CHARPIN. *ACI Cryptologie, Algorithmique et Codes.* 2002, Premier rapport d'évaluation.

[83] M. FINIASZ. *Words of Minimal Weight and Weight Distribution in Binary Goppa Codes.* submitted to ISIT 2003.

[84] C. FONTAINE. *Le tatouage des images numériques.* Pour la Science, dossier "l'art du secret", été, 2002.

[85] J. FRIEDMAN, J. TILLICH. *Generalized Alon-Boppana Theorems and Error-Correcting Codes.* submitted to SIAM Journal of Discrete Mathematics.

[86] C. NEDELOAIA. *Sur les distributions des poids des codes cycliques auto-duaux.* 2002, Journées C2 (Codes et Cryptographie) Marseille, Luminy.

[87] G. OLOCCO, J.-P. TILLICH. *A family of self-dual codes which behaves in Many Respect like random linear codes of rate 1/2.* soumis pour publication.

[88] L. PERRET. *Constructions d'instances particulières de systèmes de type Polly-Cracker.* Mémoire de DEA, Université d'Évry Val d'Essonne, 2002.

[89] P. QUANTY. *Etude d'une attaque d'un algorithme de chiffrement à flot.* Mémoire de DEA, Université de Limoges, 2002.

[90] F. RAYNAL, F. PETITCOLAS, C. FONTAINE. *Introduction à la stéganographie.* M.I.S.C., le magazine de la sécurité informatique, janvier, 2002.

[91] F. RAYNAL, F. PETITCOLAS, C. FONTAINE. *L'art de dissimuler les informations.* Pour la Science, dossier "l'art du secret", été, 2002.

[92] J. TILLICH, G. ZÉMOR. *The gaussian isoperimetric inequality and the probability of a decoding error.* submitted to IEEE Transactions on Information Theory.