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 [Détachement]
Conseiller scientifique
Guy Chassé [École des Mines de Nantes]
Collaborateurs extérieurs
Thierry Berger [Université Limoges]
Francis Blanchet [Lycée Montaigne]
Claude Carlet [Université Caen]
Éric Filiol [ESAT]
Caroline Fontaine [Université Lille]
François Laubie [Université Limoges]
Dominique Le Brigand [Université Paris 6]
Françoise Levy-dit-Vehel [ENSTA]
Pierre Loidreau [ENSTA]
Chercheur invité
Grigory Kabatianskiy [IPPI Moscou, Russie, de janvier à décembre 2001]
Ingénieurs experts
Hervé Alavoine [I.U.T. de Villetaneuse, Université Paris 13, de février 2000 à juillet 2001]

Nicolas Courtois [Université Paris 6, de novembre 2000 à avril 2001]
Doctorants
Magali Bardet-Turel [Bourse MESR, co-direction avec l'Université Paris 6, depuis septembre 2001]
Matthieu Finiasz [ENS, depuis octobre 2000]
Fabien Galand [Bourse BDI, depuis septembre 2001]
Carmen Nedeloaia [Bourse régionale, Université de Limoges, depuis septembre 2001]
Harold Ollivier [X-Telecom, depuis septembre 2001]
Gregory Olocco [Bourse MESR, co-direction avec Orsay, depuis septembre 1999]
Emmanuel Prouf [Bourse MESR, depuis septembre 1999]
Cédric Tavernier [Bourse DGA, depuis septembre 2000]
Marion Videau [Bourse DGA, depuis septembre 2001]
Stagiaires
Carlos Aguilar-Melchor [Stage de fin d'études, École Polytechnique, d'avril à juillet 2001]

Magali Bardet-Turel [Stage de DEA, Université Paris 6, d'avril à juin 2001]
Fabien Galand [Stage de DEA, Université de Caen]
Ali Lamouchi [Stage de DUT, Université de Paris 13, Villetaneuse, de juillet à août 2001]

Carmen Nedeloaia [Stage de DEA, Université de Limoges, d'avril à juin 2001]
Marion Videau [Stage de fin d'études, ENSICA de Toulouse, de mars à août 2001]

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. 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).

4 Résultats nouveaux

4.1 Étude et analyse de structures discrètes

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

[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.

des classes d'objets exceptionnels, de concevoir des outils pour les traiter, de reconnaître une structure ...

4.1.1 Groupes d'automorphismes

Participants : Thierry Berger, 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. Les chercheurs du projet ont obtenu des résultats importants dans ce domaine. Les plus marquants sont cette année la détermination des groupes d'automorphismes des codes de Reed-Muller homogènes et projectifs et un nouvel algorithme de preuve de l'équivalence de deux codes linéaires binaires (voir section suivante). T. Berger a notamment construit des codes de Reed-Muller projectifs cycliques et quasi-cycliques par le choix de systèmes de représentants de l'espace projectif compatible avec certaines permutations linéaires.

D'autre part, T. Berger s'est intéressé aux groupes d'automorphismes des codes *alternants*. Ces codes sont des sous-codes des codes de Reed-Solomon généralisés et contiennent les codes de Goppa classiques. Il a montré qu'il existe quatre classes de codes alternants cycliques et que parmi ceux-ci certains sont des codes de Goppa. Il a alors effectué une étude extrêmement fine des groupes de permutations des codes de Goppa afin d'identifier des structures particulières. Ses résultats sont importants, prolongeant notamment les travaux de H. Stichtenoth[3]. Il obtient de nouvelles familles de codes de Goppa cycliques ou d'extension cyclique. Il exhibe ainsi des codes de Goppa non cycliques dont le sous-code de poids pair est cyclique. Beaucoup parmi eux sont quasi-cycliques et ont des paramètres inconnus pour des codes quasi-cycliques. Certains atteignent les meilleures bornes connues pour des codes linéaires.

4.1.2 Codes équivalents.

Participants : Nicolas Sendrier, Gintaras Skersys.

Deux codes sont équivalents par permutation s'il existe une permutation des coordonnées de l'un le transformant en l'autre. Le problème de décision associé a été étudié récemment par Petrank et Roth [4] qui ont montré qu'il n'était pas NP-complet, mais était, en revanche, au moins aussi dur que le problème de décider de l'équivalence entre deux graphes. Trouver un algorithme efficace pour résoudre le problème de l'équivalence des codes présente donc un intérêt certain.

N. Sendrier a conçu et mis en œuvre un nouvel algorithme permettant de tester l'équivalence de deux codes linéaires donnés. Cet algorithme est capable de décider, dans presque tous les cas, de l'équivalence (par permutation) de deux codes à partir d'un invariant (*i.e.* une propriété d'un code invariante par permutation du support). Cet invariant devra pouvoir se calculer en

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

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

temps polynômial, et devra être discriminant, c'est-à-dire prendre *souvent* des valeurs distinctes pour deux codes non équivalents. La difficulté consiste à faire fonctionner l'algorithme lorsque *souvent* n'est pas très proche de *tout le temps* (par exemple une fois sur deux).

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

Les diverses applications possibles de l'algorithme, en relation avec la solidité de certains cryptosystèmes, sont présentées au §4.2.1.

Dans le cadre de sa thèse, G. Skersys a étudié avec N. Sendrier les algorithmes de calcul des groupes d'automorphismes des codes linéaires. Il a obtenu des améliorations importantes des algorithmes connus dans ce domaine. Des travaux sont en cours avec Nicolas Sendrier et ont fait l'objet d'une communication cette année lors du colloque ISIT'2001 [50].

4.1.3 Codes de Goppa

Participants : Thierry Berger, Pierre Loidreau.

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

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

P. Loidreau a construit des nouvelles familles de codes dérivés de codes de Goppa possédant certains invariants. Des bornes en distance et en dimension des codes de Goppa, on peut déduire des bornes en distance et en dimension des codes dérivés [31]. L'intérêt de cette nouvelle famille de codes est de représenter presque parfaitement les codes de Goppa dont ils sont issus, tout en étant de longueur et de dimension bien plus petites. Mais surtout cette étude aboutit à la conception d'un nouveau cryptoystème (voir §4.2.1).

4.1.4 Codes cycliques et trinômes sur un corps fini

Participants : Pascale Charpin, Pierre Loidreau.

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

Les problèmes abordés ici relèvent de la théorie des corps finis. Précisément la détermination des mots de petit poids des codes étudiés est obtenue en factorisant des classes de polynômes lacunaires. Il s'agit notamment de *trinômes*. Dans ce contexte, l'article le plus récent porte sur les classes de *suites binaires qui ont la propriété du trinôme*. Ce sont des suites dont les symboles vérifient un ensemble d'équations courtes (ici trois termes) [28].

L'étude des codes cycliques primitifs est étroitement liée à l'étude de certaines suites binaires ou encore des permutations utilisées dans le chiffrement par blocs. Les travaux des chercheurs du projet sur ce thème sont décrits plus loin (voir §4.5).

4.1.5 Théorie des nombres, algèbre finie

Participant : François Laubie.

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

Ses travaux cette année ont porté d'une part sur les systèmes dynamiques nonarchimédiens (avec A. Salinier et A. Movahhedi) et d'autre part sur les suites binaires minimalement autocorrélées (avec M. Bauderon).

4.2 Cryptographie à clé publique

4.2.1 Système de chiffrement utilisant des codes correcteurs

Participants : 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.

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

Jusqu'à ce jour, il n'y avait pas de résultat connu sur l'attaque par structure du système de McEliece basé sur les codes de Goppa classiques. La structure des codes de Goppa semble suffisamment complexe, la classe suffisamment large. Dans ce contexte, P. Loidreau et N. Sendrier ont réalisé une avancée importante en isolant des classes de codes de Goppa qui possèdent certains invariants, des isomorphismes de corps. Il s'agit d'une application remarquable de l'algorithme de *séparation du support* de N. Sendrier (cf. §4.1.2). L'ensemble de ces travaux sur le système de chiffrement de McEliece a été présenté dans une conférence invitée au *Workshop on Coding Theory and Data Integrity* à Singapour [51].

P. Loidreau a étudié la possibilité de réduire la taille des clés tout en gardant une sécurité suffisante. Il a montré, pour le cryptosystème de McEliece, qu'il est possible d'accroître la sécurité contre l'attaque par décodage aléatoire en utilisant des propriétés algébriques du groupe d'automorphismes. On peut ainsi développer des schémas cryptologiques plus résistants aux attaques connues. Il s'est intéressé à d'autres types de systèmes tels les systèmes MRD découverts par E. M. Gabidulin mettant en œuvre de nouveaux outils mathématiques et algorithmiques. L'aspect décodage de ces codes repose en effet sur une métrique différente de la métrique de Hamming classique utilisée jusqu'à présent ; ceci est le point de départ d'une étude avec E. M. Gabidulin [44].

T. Berger et P. Loidreau ont étudié plus généralement la notion d'ensemble d'erreurs corrigibles qui ne sont plus en relation directe avec la métrique de Hamming.

4.2.2 Système de signature utilisant des codes correcteurs

Participants : Nicolas Courtois, Nicolas Sendrier, Matthieu Finiasz.

Il a été possible de réaliser un algorithme de signature fondé sur les principes du système de chiffrement à la clé publique de McEliece (camouflage d'une structure de code décodable). Cette méthode possède tous les avantages du système de McEliece (sécurité, rapidité de vérification ...) et a en plus l'avantage de donner des signatures très courtes. En effet, grâce à lui, il est possible de prouver à la fois l'origine et le contenu d'un document avec seulement 81 bits de signature. Obtenir un résultat équivalent du point de vue de la sécurité avec le système RSA nécessite une signature de 1024 bits.

Ce résultat devrait donc donner un nouveau souffle de vie, au système de McEliece, et plus généralement à tous les cryptosystèmes reposant sur des codes correcteurs d'erreurs. Ce travail réalisé en commun par Nicolas Sendrier, Matthieu Finiasz et Nicolas Courtois a déjà donné lieu à une publication à la conférence ASIACRYPT 2001 [43].

4.2.3 Cryptosystèmes basés sur des problèmes combinatoires et algébriques

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

On s'intéresse ici aux systèmes de chiffrement qui sont de nature algébrique, mais dont la clef publique (constituée d'un ensemble de polynômes), est construite à partir de problèmes difficiles de combinatoire. L'exemple générique de tels systèmes est connu sous le nom de Polly-Cracker. Plusieurs problèmes se posent dans ce contexte : comment construire une instance sûre d'un tel schéma, comment améliorer le taux de chiffrement, trouver des constructions effectives ...

Cette activité, débutée en septembre 2001, est menée dans le cadre de l'*action concertée incitative ACCES (outils Algébriques et Combinatoires pour la Construction et l'Etude de Systèmes à clef publique)*, dirigée par F. Levy-dit-Vehel. Pierre Loidreau et Patrick Ciarlet (enseignant-chercheur HDR à l'ENSTA depuis 97) font également partie de cette ACI. Patrick Ciarlet intervient principalement sur des aspects d'algorithmique en lien avec des problèmes de théorie des graphes sous-jacents à la construction de clefs publiques. Pierre Loidreau contribue à l'étude des polynômes dans les corps finis. Étant donné le lien fort entre la sécurité des schémas

Polly-cracker et la résolution d'équations algébriques sur un corps fini (la clef publique doit par exemple être résistante à des attaques consistant à en trouver une base de Gröbner), les chercheurs impliqués ont initié une collaboration avec les membre de l'ACI POLYCRYPT.

4.2.4 Courbes elliptiques et autres courbes

Participants : Daniel Augot, Guy Chassé, Cédric Tavernier.

Ces dernières années, l'évolution des logiciels de calcul formel et le développement du thème *Géométrie algébrique et codage*, ont amené les chercheurs à formuler d'importants problèmes de recherche en terme de résolution de systèmes d'équations sur les corps finis. Il en est ainsi pour la détermination de mots de poids faible pour certains codes correcteurs. Dans le même temps s'est développée la cryptologie basée sur les courbes elliptiques, proposant une technologie globalement plus efficace que RSA.

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

L'*action de recherche coopérative* (ARC) « COURBES » dirigée par Daniel Augot[5] a été initiée en Juin 1999. Elle regroupe trois équipes ayant des compétences complémentaires : le projet CODES, le LIX (École polytechnique) et le LACO (Université de Limoges). Les deux principaux axes de recherche sont :

- analyse des courbes elliptiques et hyperelliptiques – cryptanalyse des systèmes existants ;
- recherche et étude de nouvelles courbes – conception et optimisation de cryptosystèmes.

Daniel Augot et Guy Chassé étudient actuellement l'arithmétique des courbes C_{ab}. On sait maintenant bien calculer dans le groupe des points d'une courbe elliptique, et la question naturelle est d'étudier d'autres courbes dont le groupe associé est le groupe de Picard, ou jacobienne. En effet divers isomorphismes existent entre les courbes, et tout progrès pour les courbes générales peut conduire à des attaques sur les cryptosystèmes à base de courbes elliptiques.

Cédric Tavernier a étudié une nouvelle approche pour déterminer le nombre de points d'une courbe elliptique [52]. G. Frey et M. Müller en 1998, ont utilisé $X_0(N)$ et les nouvelles formes pour en déduire la cardinalité des variétés abéliennes modulaires sur F_p. Cette approche repose sur la théorie des symboles modulaires et donc sur les résultats de Merel, Manin, Shokurov, Shimura, Crémona. Mais il s'avère que la complexité est exponentielle, et que cette méthode ne peut convenir en utilisation cryptographique.

4.3 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

[5] `http://www-rocq.inria.fr/codes/Daniel.Augot/courbes`

codes *résidus quadratiques*. La deuxième est l'apparition de nouvelles applications en correction d'erreurs et en cryptologie.

L'étude des performances des *petits codes correcteurs en bloc* est d'actualité à cause du développement de systèmes où l'information est transmise *par paquets* de petites longueurs. Le but recherché actuellement est de concevoir des systèmes où la rapidité avoisinerait celle obtenue lorsque l'on effectue une correction en ligne. Le projet a commencé à développer ce thème de recherche par l'étude de nouveaux codes, dits *codes CORTEX* dans le cadre d'un contrat (voir § 5). Ces codes sont construits à partir d'un ensemble de codes de longueur 8 ou 4, concaténés et entrelacés. Les codes CORTEX sont autoduaux. G. Olocco et J.-P. Tillich ont obtenu des résultats surprenants sur le comportement asymptotique de cette propriété [66] ; ils ont proposé un algorithme itératif de décodage adapté à ces codes.

L. Pecquet étudie, pour sa thèse, l'algorithme de Sudan. Cet algorithme, dit *de décodage par liste*, suscite un vif intérêt dans la communauté du codage, car il présente un paradigme nouveau pour décoder. Il s'agit d'un décodage par interpolation plutôt que par calcul de syndromes.

Dans le cadre du décodage des codes géométriques, L. Pecquet a étendu l'algorithme de décodage de Sudan pour le contexte plus général d'un canal à information souple[6]. Ces travaux sont fondés sur la reconstruction de fonctions géométriques. L'accent a été mis sur l'algorithmique des courbes planes et des codes géométriques pour rendre effectives et efficaces les méthodes de reconstruction et de décodage. L'implantation des codes géométriques réalisée l'année passée dans le système MAGMA a été améliorée et les méthodes de décodage ont également été implantées. Lancelot Pecquet soutiendra ta thèse en décembre.

Daniel Augot et Magali Bardet-Turel ont étudié, dans le cadre d'un stage de DEA, le décodage des codes cycliques en utilisant les bases de Groebner, en collaboration avec Jean-Charles Faugère du projet SPACES. Il s'agit de décoder les codes à résidus quadratiques, pour lesquels aucun algorithme de décodage général n'est connu. Les travaux ont montré qu'il est possible de décoder par calcul de base de Groebner, avec une bonne performance. Il est aussi possible de décoder au-delà de la distance minimale [55].

4.4 Décodage et cryptanalyse

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

Suite à de nombreux travaux récents, il est bien connu que les algorithmes de décodage sont des outils performants en cryptanalyse[7]. 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 ré-

[6] Une telle extension a été présentée par Kötter et Vardi au colloque ISIT'2000 pour le décodage des codes de Reed-Solomon.

[7] Le projet s'est investi depuis longtemps dans ce domaine de recherche [4]

troaction 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.

4.5 Primitives du chiffrement symétrique

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

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*.

4.5.1 Haute non-linéarité et critère de propagation.

Une fonction est de *haute non-linéarité* lorsqu'elle se situe à grande distance de l'espace $R(1,m)$ des fonctions affines de m variables. Cela signifie qu'elle définit un translaté de l'espace

$R(1,m)$ de poids de Hamming élevé. La notion de *fonction courbe*, introduite en 1975, désigne les fonctions booléennes de non-linéarité maximum, 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. La non-linéarité des fonctions booléennes est étroitement liée au concept de *confusion*, défini par C. Shannon [8], essentiel pour garantir la sécurité d'un système de chiffrement. Parallèlement, le second critère de fiabilité en cryptographie est celui de *diffusion*. Cette notion signifie, dans le cas du chiffrement par blocs par exemple, qu'une faible modification en entrée est diffusée dans l'ensemble du bloc de sortie. Ce critère correspond au *critère de propagation* pour les fonctions.

A. Canteaut, C. Carlet, P. Charpin et C. Fontaine ont étudié les relations entre ces deux critères fondamentaux. L'objet de ce travail était de mettre en place une série d'outils théoriques et algorithmiques qui permettent d'obtenir de nouveaux éléments de description ou classification. Ce travail s'est révélé extrêmement fructueux et un grand nombre de résultats fondamentaux sont apparus. D'autres critères, tels la *résilience*, interviennent et sont mis en évidence. L'ensemble de ces résultats a été publié en tant que *regular paper* dans la revue IEEE-IT [21]. Par ailleurs, A. Canteaut a obtenu des résultats précis sur la distribution des poids de certains translatés optimaux de $R(1,m)$ [24].

C. Carlet a, dans sa conférence invitée à Fq6 (*Finite Fields and their Applications*, Oaxaca, Mexique, Mai 2001) [41] et dans l'article qu'il a soumis aux proceedings [62], montré que presque toutes les fonctions booléennes sont de haute complexité vis-à-vis de plusieurs critères tels que la non-linéarité, le nombre minimal de termes dans les formes algébriques normales des fonctions équivalentes, le degré algébrique et la non-normalité (i.e. l'inexistence d'un sous-espace affine de l'espace des mots binaires de longueur n sur lequel la fonction soit affine et dont la dimension soit bornée inférieurement en $O(\log n)$). 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* [60]).

4.5.2 Fonctions courbes

A. Canteaut et P. Charpin ont mis en évidence de nouvelles propriétés concernant les restrictions des fonctions courbes à des sous-espaces affines. Cette étude montre notamment que les fonctions courbes diffèrent de par la structure de leurs décompositions en 4 fonctions. Les premiers résultats de ce travail ont été présentés dans une conférence invitée lors du *Workshop on Coding Theory and Data Integrity* à Singapour [35].

C. Carlet a mis en évidence, avec Andrew Klapper, deux bornes supérieures efficaces sur les nombres de fonctions courbes et résilientes [61].

[8] C. Shannon - *Communication theory of secrecy systems* - *Bell system technical journal*, vol. 28, pp. 656-715 (1949).

4.5.3 Fonctions vectorielles presque courbes, presque parfaitement non-linéaires et chiffrement à clé secrète

L'algorithme DES était, jusqu'à récemment, considéré comme solide puisqu'on ne dispose d'aucune technique de cryptanalyse qui soit sensiblement plus efficace que l'énumération de toutes les clefs possibles. Toutefois, comme sa clef secrète ne comportait que 56 bits, le DES est devenu vulnérable à une recherche exhaustive de la clef. C'est pourquoi un nouvel algorithme de chiffrement par blocs, dit *Advanced Encryption Standard* (AES), vient d'être standardisé[9], Joan Daemen et Vincent Rijmen.
`http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`. Il était nécessaire de remplacer la fonction de confusion du DES (spécifiée par les boîtes S) par une permutation définie sur un corps fini d'ordre plus élevé. Cette permutation doit de plus vérifier certains critères afin que le système de chiffrement résiste aux attaques classiques dont les principales sont la cryptanalyse linéaire et la cryptanalyse différentielle. Pour se prémunir de ces attaques, on utilise des fonctions *presque parfaitement non linéaires* et *presque courbes* car elles assurent une résistance optimale aux cryptanalyses différentielle et linéaire. Ces propriétés apparaissent également dans l'étude des suites de longueur maximale puisque les fonctions puissances (i.e. $x \mapsto x^d$) presque courbes coïncident avec des couples de *suites de longueur maximale dont la corrélation croisée est optimale.*

Il est montré dans [7] que les fonctions presque courbes correspondent à des codes linéaires dont la distribution des poids est optimale. Dans le cas des fonctions puissances, ces codes sont en fait les duaux de certains codes cycliques à deux zéros. Grâce à cette analogie, A. Canteaut, P. Charpin et H. Dobbertin ont prouvé que les fonctions presque courbes sont entièrement caractérisées par la distance duale et la divisibilité des poids du code qui leur est associée. Ceci leur a notamment permis de démontrer une conjecture formulée par Welch en 1968, selon laquelle la fonction $x \mapsto x^d$, où $d = 2^{(m-1)/2} + 3$, est presque courbe sur $\mathbf{F}_{2^m}$ quand m est impair. L'ensemble de ces travaux fait l'objet d'une conférence invitée à *Indocrypt 2001* [38].

Par ailleurs, A. Canteaut et M. Videau ont mis en valeur l'importance de la divisibilité des coefficients de Fourier des fonctions utilisées dans les systèmes de chiffrement itératifs par blocs. Ce paramètre essentiel permet en particulier d'évaluer la résistance du système aux attaques différentielles d'ordre supérieur [69, 58]. Elles ont notamment montré que la permutation $x \mapsto x^{-1}$ dans le corps d'ordre 256, qui a été choisie pour l'AES, était la seule fonction de non-linéarité optimale assurant une bonne résistance à ces attaques. En effet, les coefficients de Fourier de cette permutation possèdent la plus faible divisibilité possible.

4.5.4 Fonctions t-résilientes

Les fonctions t-résilientes forment une classe de fonctions booléennes très utilisées en cryptographie, en particulier pour l'assemblage des sorties de registres à décalage pour le chiffrement par flot. Elles interviennent également dans la conception de nombreuses primitives conventionnelles telles les fonctions de hachage. C. Carlet a introduit en collaboration avec Y. Tarannikov la notion de *séquence couvrante des fonctions booléennes.* Cette notion fait intervenir les dérivées de la fonction. Elle est ainsi naturellement liée au critère de propagation d'une part, et à la

[9] **AES Proposal : Rijndael**

notion de fonction courbe (i.e. de non-linéarité maximale) d'autre part (ces dernières fonctions sont caractérisées par le fait que toutes leurs dérivées sont équilibrées). Ils ont montré que les critères de non-corrélation et de résilience peuvent être caractérisés par l'existence de certaines séquences couvrantes. Le rôle des dérivées relativement à ces critères est ainsi avéré. De plus, en considérant des séquences couvrantes particulières, ils ont exhibé des sous-classes de fonctions résilientes aux propriétés de non-linéarité intéressantes. Ils ont donné des constructions de telles fonctions dont les non-linéarités atteignent les bornes supérieures connues. Leur article va paraître dans la revue *Designs, Codes and Cryptography* [26].

Grâce à l'utilisation d'une représentation des fonctions booléennes qu'il a introduit avec Philippe Guillot et qui permet une caractérisation des fonctions résilientes et des fonctions sans corrélation, C. Carlet a par ailleurs montré une nouvelle borne supérieure sur la non-linéarité de ces fonctions. Cette borne améliore la récente borne mise en évidence parallèlement par Maitra-Sarkar, Tarannikov et Zheng-Zhang. Elle fait intervenir non seulement l'ordre de résilience (resp. de non-corrélation) de la fonction et le nombre des variables qu'elle met en jeu, mais aussi le degré algébrique de la fonction. C'est l'intervention du degré algébrique qui permet de faire baisser (d'une façon importante dans la majorité des cas) la valeur de cette borne supérieure. Ce travail a été publié sous forme de résumé long dans les comptes rendus de l'Académie des Sciences [27] et sous forme d'article complet dans les actes du congrès SETA'01 (Sequences and their Applications) [42]. C. Carlet a ensuite obtenu avec Palash Sarkar une deuxième preuve de cette même borne, basée sur les seules propriétés de la transformée de Fourier [25].

4.5.5 Chiffrement COS

Caroline Fontaine, E. Filiol et D. Vianne (Centre de Recherche des Écoles de Coëtquidan & INRIA) ont mis au point une nouvelle famille de systèmes de chiffrement par blocs, COS (pour *Crossing Over Systems*). L'idée générale de ce schéma est de combiner les avantages du chiffrement par blocs avec ceux du chiffrement à flot, en évitant leurs inconvénients respectifs. Quelques rares travaux avaient présenté des fonctions de hachage (avec clef) ou des schémas de chiffrement par blocs utilisant des éléments de chiffrement à flot. C'est cette idée que nous avons développée.

Les éléments de base du système sont des registres à décalage dont la rétroaction n'est pas linéaire. Chaque rétroaction est définie par une fonction booléenne ; celes choisies sont celles générées pendant la thèse de Caroline Fontaine : elles satisfont en effet toutes les propriétés requises, et leur spectre de Fourier est particulièrement plat, ce qui rend les attaques plus difficiles (il n'y a pas de biais à exploiter). Nous avons élaboré une construction originale, nommée *crossing over*, qui permet d'utiliser les états internes des registres comme parties pour les blocs de sortie du système de chiffrement.

De nombreux tests statistiques (extraits pour la plupart du livre de D. Knuth) ont été mis en place pour évaluerer le comportement de notre système, et ont tous donné satisfaction.

Deux articles publient ces résultas [45, 46] en montrant la grande rapidité de COS. Un défi cryptographique est même lancé.

4.6 Chiffrement symétrique : cryptanalyse

Participants : Anne Canteaut, Éric Filiol, Marion Videau.

A. Canteaut et M. Videau ont montré que certains chiffrements symétriques par blocs, qui résistent aux attaques différentielles et linéaires, sont vulnérables à des attaques différentielles d'ordre supérieur (*cf.* §4.5.3).

Par ailleurs, les chercheurs du projet ont élaboré des cryptanalyses efficaces des générateurs pseudo-aléatoires basés sur des registres à décalage à rétroaction linéaire. Outre l'attaque par décodage présentée dans §4.3, plusieurs techniques ont été mises au point par A. Canteaut et É. Filiol.

La première, dite *attaque par décimation de la suite de sortie*, consiste en une *transformation de schéma* opérée sur le système : un ou plusieurs registres sont remplacés par un ou des registres plus courts. Ceci est réalisable dès que le degré du polynôme de rétroaction correspondant n'est pas un nombre premier. Cette attaque, qui met en lumière des failles dans les choix des paramètres du système, est plus efficace quand les registres sont longs (comparée à d'autres attaques) [47].

La deuxième attaque concerne plus particulièrement les *registres filtrés*, dans lesquels la suite pseudo-aléatoire produite correspond à la sortie d'une fonction booléenne non-linéaire dont les entrées sont certaines cellules d'un registre à décalage à rétroaction linéaire. A. Canteaut et E. Filiol ont exhibé une nouvelle attaque de ces systèmes, qui généralise les attaques par corrélation rapides. Ils ont notamment montré que les propriétés spectrales et le nombre de variables de la fonction de filtrage n'influençaient pas les performances de l'attaque. Les premiers résultats de ces travaux font l'objet d'un article soumis à la conférence *Fast Software Encryption 2002* [57].

Enfin, A. Canteaut et É. Filiol ont également conçu un algorithme de *reconstruction* des systèmes de chiffrement à flot qui utilisent (pour cacher le texte clair) un générateur pseudo-aléatoire à combinaison de registres. Connaissant la représentation du « clair » et admettant que le temps de reconstruction peut être « long », puisqu'effectué une fois pour toutes, les polynômes de rétroaction puis la fonction de composition, sont révélés. Cette attaque relève de la problématique suivante : faut-il, ou non, pour renforcer la sécurité d'une chaîne de transmission, dissimuler les algorithmes de codage ? [36].

Magali Bardet-Turel démarre une thèse intitulée « Cryptanalyse du système HFE (Hidden Field Equations), et aspects algébriques des cryptosystèmes ». Le système HFE est un cas typique de cryptosystème algébrique, qui peut s'attaquer par résolution de système d'équations. Le cryptosystème résiste à l'attaque menée directement, il faut donc améliorer et adapter les algorithmes de calcul de bases de Groebner dans le cas des corps finis. Co-encadrée par Daniel Augot et Jean-Charles Faugère, Magali étudiera la cryptanalyse de HFE, ainsi que les problèmes particuliers du calcul des bases de Groebner sur les corps finis. Ces thèmes font l'objet d'une ACI crypto, baptisée Polycrypt, dirigée par Guillaume Hanrot, du projet SPACES.

4.7 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.

4.8 Protection des droits d'auteurs – watermarking

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

Suite aux travaux sur le projet européen AQUARELLE, qui ont donné lieu à [1] sur les techniques de marquage d'images, 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 [29]. 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 est presente a la conference Electronic Imaging [49] en janvier 2002.

Françoise Levy-dit-Vehel participe au projet RNRT DIPHONET (DIffusion de PHOtographies à travers (I)nterNET - projet précompétitif, labellisé[10] 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).

[10] urlhttp ://www.telecom.gouv.fr/rnrt/index_net.htm

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).

– 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.

5 Contrats industriels (nationaux, européens et internationaux)

Nous décrivons dans ce paragraphe nos activités de transfert scientifique et développement. Une étude pour le CCETT de Rennes portant sur les codes CORTEX (voir §4.3), débutée fin 99, s'est poursuivie en 2001. Par ailleurs, le projet a travaillé sur un contrat PRIAMM portant sur le marquage des films.

5.1 Collaboration CNET/INRIA+LACO

Étude de nouveaux turbo-codes en bloc, les codes CORTEX, 99-2001.
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 § 4.3).

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.

5.2 Projet iFIC (PRIAMM) 2000–01

Le projet iFIC (internet Films of Independent Cinema), d'une durée de 18 mois à partir d'avril 2000, comporte quatre partenaires, la société Pangea Web Diffusion, l'Institut National des Télécommunications, l'École polytechnique (LIX), et l'INRIA (CODES). Le but est la diffusion sur internet d'œuvres du cinema indépendant français. Le projet CODES est responsable des aspects sécurité, ce qui nécessite la conception d'un système de chiffrement spécifique (à très haut débit), ainsi que d'un système de marquage d'images ayant pour but de dissuader les éventuels fraudeurs. Deux ingénieurs experts ont été embauchés pour ce contrat, Hervé Alavoine pour un an (de juillet 2000 à juillet 2001) et Nicolas Courtois pour six mois (d'octobre 2000 à mars 2001).

6 Actions régionales, nationales et internationales

6.1 Actions nationales

Collaboration scientifique et échanges se sont poursuivis en 2001, 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. Nous avons besoin de spécialistes en théorie de groupes finis (T. Berger), en théorie algébrique des nombres (F. Laubie) et en géométrie algébrique (D. Le Brigand). Ceci se concrétise par des travaux en commun ou des co-directions de thèses.

6.1.1 Contrats nationaux

– **Action de recherche coopérative « COURBES »** (Juin 99-Juin 2001). Le responsable est D. Augot. Les équipes membres sont le projet CODES à l'INRIA, le LIX à l'École polytechnique (F. Morain). L'Université de Limoges a fait défaut, avec le départ d'Yvan Duursma. Le thème de recherche est celui de l'étude des courbes algébriques et leur utilisation pour la cryptographie[11].

– **Action Concertée Incitative « Cryptologie »**. Notre projet, soumis au premier appel d'offre (Septembre 2000) a été retenu dans le cadre du *soutien aux équipes d'excellence* pour un financement de trois ans.

[11] `http://www-rocq.inria.fr/codes/Daniel.Augot/courbes/une.html`

Titre : *Cryptologie, Algorithmique et Codes* ;
Coordinateur du projet : Pascale Charpin ;
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. Notre action s'inscrit dans le long terme autour de problèmes jugés difficiles, comme l'identification de nouveaux critères de conception des systèmes à clé secrète ou la conception d'un algorithme de signature digitale utilisant des codes correcteurs ou encore l'élaboration de nouvelles cryptanalyses par décodage.

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 »**. Un deuxième projet a été soumis au deuxième appel d'offre (Juillet 2001) ; il a été retenu pour un financement de trois ans.
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.

6.1.2 Groupes de recherche

Le projet participe à deux groupements de recherche nationaux :
- GDR *Algorithmique, Modèles, Infographie* (AMI) en reconstruction, équipe *Protection des Communications*, responsable Claude Carlet.

Dans le cadre du GDR AMI, Claude Carlet a 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.

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[12] depuis octobre 99.

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

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

6.1.3 Participations à des instances et manifestations nationales

Plusieurs membres du projet participent à des commissions de spécialistes :
- Université de Caen, 27$^{\text{ème}}$ section (cnu) : C. Carlet.
- Université de Limoges, 25$^{\text{ème}}$ section (cnu) : T. Berger, A. Canteaut, C. Carlet, P. Charpin, F. Laubie.
- Université du Var, 27$^{\text{ème}}$ section (cnu) : C. Carlet, P. Charpin.
- Université Paris 6, 25$^{\text{ème}}$ section (cnu) : D. Le Brigand.
- INRIA-Rocquencourt, section d'audition du jury CR2 2001 : P. Charpin.

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

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

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

6.2 Actions internationales

6.2.1 Organisation de rencontres, expertises

Le projet participe régulièrement à l'expertise des travaux de recherche pour les revues ou conférences internationales. On peut citer notamment pour cette année, les revues *IEEE on Information Theory*, *IEEE on 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 :
- C. Carlet et P. Charpin sont membres du comité de programme de *14th International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes* (AAECC14), Melbourne, Australie, Novembre 2001.
- C. Carlet est membre du comité de programme de *Indocrypt*, Madras, Inde, Décembre 2001.
- A. Canteaut est membre du comité de programme de la conférence *YACC 2002*, Porquerolles, France, juin 2002.
- Les membres du projet démarrent la préparation du colloque international *Workshop on Coding and Cryptography 2003*, qui aura lieu à Paris. Le comité de programme est présidé par C. Carlet et le comité d'organisation par N. Sendrier (cf. `http://www-rocq.inria.fr/codes/WCC2001`).
- **Spécial issue in Coding and Cryptography**, Éditeur : Claude Carlet, à paraître dans la revue Discrete Applied Mathematics.

6.2.2 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 2001 :
- Ernst Gabidulin (Institut de Physique et de Technologies, Moscou, Russie) ;
- David Haccoun (École Polytechnique de Montréal, Québec, Canada) ;
- Enes Pasalic (Lund University, Suède) ;

– Gintaras Skersys (Université de Vilnius, Lituanie).

7 Diffusion de résultats

7.1 Enseignement

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

– Daniel Augot intervient dans le module Programmation de licence informatique de Paris VI. Renaud Rioboo et Thérèse Hardin ont défini le projet FOC[13], dont le but est de construire un système de calcul formel expérimental, en utilisant les connaissances acquises en sémantique des langages de programmation. Les bases de ce système sont celles d'Objective Caml, et l'objectif est de produire un système aussi riche et plus performant qu'Axiom. Daniel Augot s'implique dans cet enseignement, à but d'auto-apprentissage sur Caml et la sémantique, pour comprendre le projet FOC.
– 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.
– 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,

– A. Canteaut et C. Fontaine ont donné deux conférences, intitulées respectivement *Introduction à la cryptographie* et *Protection des droits d'auteur pour les documents numériques*, dans le cadre du séminaire X-Aristote consacré à la sécurité des transactions et des sites informatiques (octobre 2001).
– A. Canteaut et F. Lévy-dit-Véhel ont rédigé un article introductif aux techniques cryptographiques paru dans la revue *L'Armement* [22, 23].

7.2 Jurys de thèse

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

[13] `http://calfor.lip6.fr/~foc`

Novembre 00 H. Massias,
La certification cryptographique du temps,
Thèse d'Université en cotutelle Louvain-Limoges.
Jury : T. Berger (co-président).

Novembre 00 S. Semirat,
Problèmes de nombres de classes pour les corps de fonctions et application,
Thèse d'Université de Paris 6.
Jury : D. Le Brigand (direction).

Mars 01 S. Penaud,
Étude des potentialités du chaos pour les systèmes de télécommunications. Évaluation des performances de systèmes DS-CDMA utilisant des séquences d'étalement chaotiques,
Thèse d'Université de Limoges.
Jury : T. Berger.

Mars 01 É. Filiol,
Techniques de reconstruction en cryptologie et théorie des codes,
École polytechnique.
Jury : P. Charpin (direction), C. Carlet, G. Kabatiansky.

Mai 01 P. Loidreau,
Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs,
École polytechnique.
Jury : P. Charpin (direction), T. Berger, G. Kabatiansky (rapporteurs), N. Sendrier.

Juin 01 S. Dubuc Camus,
Étude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non linéaires,
Thèse d'Université de Caen.
Jury : A. Canteaut, C. Carlet (direction), P. Charpin (rapporteur).

Juillet 01 C. Brunie,
Étude et preuve de la faisabilité de l'approche combinée fraction continue / sous-résultants symétriques, implantation sur la machine de Turing TP de Shönhage, et applications,
Thèse d'Université de Limoges.
Jury : T. Berger.

Septembre 01 N. Courtois,
La sécurité des primitives cryptographiques basées sur des problèmes algébriques multivariables : MQ, IP, MinRank, HFE.
Thèse d'Université de Paris 6.
Jury : P. Charpin.

Décembre 01 L. Pecquet,
Décodage en liste des codes géométriques,
Thèse d'Université de Paris 6.
Jury : D. Augot, P. Charpin (co-direction), C. Carlet.

7.3 Participation à des colloques

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

Séjours courts dans des universités ou laboratoires en 2001 :

- CODING THEORY AND DATA INTEGRITY, Juillet-Décembre 2001, Université de Singapour : C. Carlet, P. Charpin et N. Sendrier ont été invités (respectivement en Juillet, Août et Septembre) par H. Niederreiter (responsable de l'institut de mathématiques, organisateur de cette manifestation).

Participations aux colloques en 2001 :

- RSA *Conference*, San Francisco, USA, 8-12 avril 2001.
  Conférencier invité : N. Courtois.
- *Colloque Algorithmique et Programmation*, Luminy, France, 5-8 mai 2001.
  Participant : N. Sendrier.
- *Congrès* AGCT'8, CIRM-Luminy, France, mai 2001.
  Participante : D. Le Brigand.
- *Fq6 - Finite Fields and their Applications*, Oaxaca, Mexique, 21 au 25 mai 2001.
  Conférencier : C. Tavernier.
  Conférencier invité : C. Carlet.
- SETA'01 - *Sequences and their Applications*, Bergen, Norvège, mai 2001.
  Conférencier : C. Carlet.
- ISIT'01 - *IEEE International Symposium on Information Theory*, Washington, USA, 22-28 juin 2001.
  Conférenciers : É. Filiol, N. Sendrier, C. Fontaine, G. Olocco, J.P. Tillich.
- *Workshop on Mathematical foundations of Coding Theory and Cryptology*, Singapour, Juillet 2001.
  Conférencier invité : C. Carlet.
- *Workshop on Coding and Cryptography*, National University of Singapore, 10 - 13 Septembre 2001.
  Conférenciers invités : P. Charpin, N. Sendrier.
- *AAECC 14*, Melbourne, Australie, 26-30 novembre 2001.
  Conférencier : T. Berger.
  Participants : J.-P. Tillich (Organising Committee Information), G. Olocco.
- *Asiacrypt'01*, Brisbane, Australie, 9-13 décembre 2001.
  Conférencier : M. Finiasz.
  Participant : N. Sendrier.
- *Eighth IMA International Conference on Cryptography and Coding*, Cirencester, UK, 17-19 décembre 2001.
  Conférenciers : É. Filiol C. Fontaine.
  Participants : F. Galand, P. Loidreau.
- *Indocrypt'01*, Madras, Inde, 16-20 décembre 2001.
  Conférencière invitée : A. Canteaut.

8 Bibliographie

Ouvrages et articles de référence de l'équipe

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

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

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

[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 », *IEEE Transactions on Information Theory 44*, 1, janvier 1998, p. 367–378.

[5] A. Canteaut, P. Charpin, H. Dobbertin, « Binary m-sequences with three-valued crosscorrelation : A proof of Welch conjecture », *IEEE Transactions on Information Theory 46*, 1, 2000, p. 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 », *SIAM Journal on Discrete Mathematics 13*, 1, 2000, p. 105–138.

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

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

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

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

[11] 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.

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

Livres et monographies

[13] C. Carlet (éditeur), *Special issue in Coding and Cryptography*, Revue Applied Discrete Mathematics, 2000, Éditeurs associés : P. Charpin (INRIA-Rocquencourt), M. Girault (SEPT-Caen), G. Kabatiansky (IPPI-Moscou, H. van Tilborg (Eindhoven), à paraître.

Thèses et habilitations à diriger des recherches

[14] N. Courtois, *La sécurité des primitives cryptographiques basées sur des problèmes algébriques multivariables : MQ, IP, MinRank, HFE*, thèse de doctorat, Université de Paris 6, septembre 2001.

[15] S. Dubuc, *Étude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non linéaires*, thèse de doctorat, Université de Caen, juin 2001.

[16] É. Filiol, *Technique de reconstruction en cryptologie et théorie des codes*, thèse de doctorat, École Polytechnique, mars 2001.

[17] P. Loidreau, *Étude et optimisation de cryptosystèmes à clé publique fondés sur la théorie des codes correcteurs*, thèse de doctorat, École Polytechnique, mai 2001.

[18] L. Pecquet, *Construction et décodage des codes géométriques*, thèse de doctorat, Université de Paris 6, décembre 2001.

Articles et chapitres de livre

[19] D. Augot, L. Pecquet, « A lifting method to replace factorization in Sudan's algorithm », *IEEE Transactions on Information Theory 46*, 7, 2001, p. 2605–2614.

[20] T. Berger, « Automorphism groups of homogeneous and projective Reed-Muller codes », *ieee*, 2001, accepté pour publication.

[21] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, « On Cryptographic Properties of the Cosets of $R(1,m)$ », *IEEE Transactions on Information Theory 47*, 4, 2001, p. 1494–1513, Regular Paper.

[22] A. Canteaut, F. Lévy-dit-Véhel, « La cryptologie moderne (1) », *L'Armement 73*, mars 2001, p. 76–83.

[23] A. Canteaut, F. Lévy-dit-Véhel, « La cryptologie moderne (2) », *L'Armement 74*, juin 2001, p. 139–142.

[24] A. Canteaut, « On the Weight Distributions of optimal cosets of the First-Order Reed-Muller Code », *IEEE Transactions on Information Theory 47*, 1, 2001, p. 407–413.

[25] C. Carlet, P. Sarkar, « Spectral domain analysis of correlation immune and resilient Boolean functions », *Finite fields and Applications*, 2001, à paraître.

[26] C. Carlet, Y. Tarannikov, « Covering sequences of Boolean functions and their cryptographic significance », *Designs, Codes and Cryptography*, 2001, à paraître.

[27] C. Carlet, « On the divisibility properties and nonlinearity of resilient functions », *Comptes Rendus de l'Académie des Sciences de Paris*, t. 331, Serie 1, 2000, p. 917–922.

[28] P. Charpin, A. Tietavainen, V. Zinoviev, « On binary cyclic codes with codewords of weight three and binary sequences with the trinomial property », *IEEE Transactions on Information Theory 47*, 1, 2001, p. 421–425.

[29] F.A. Petitcolas, C. Fontaine, J. Dittmann, M. Steinebach, N. Fates, « Public automated web-based evaluation service for watermarking schemes : Stirkark benchmark », *Proceedings of the SPIE 4314*, 2001, p. 575–584, IS&T/SPIE International Symposium on Electronic Imaging 2001 : Security and Watermarking of Multimedia Contents III.

[30] P. Loidreau, N. Sendrier, « Weak keys in McEliece public-key cryptosystem », *IEEE Transactions on Information Theory 47*, 3, avril 2001, p. 1207–1212.

[31] P. Loidreau, « Codes derived from binary Goppa codes », *Problemy Peredachi Informatsii*, 2001, à paraître.

[32] A. Valembois, « Detection and recognition of a binary linear code », *Discrete Applied Mathematics 111*, 2001.

Communications à des congrès, colloques, etc.

[33] T. Berger, L. de Maximy, « Cyclic Projective Reed Muller codes », *in : Proceedings of AAECC14, (Novembre 2001)*, Melbourne, Australie, 2001.

[34] E. Cadic, J.C. Carlach, G. Olocco, A. Otmani, J.P. Tillich, « Minimal Tail-Biting Treillises of Extremal Binary and Quaternary Self-Dual Codes of Length 24, 32 and 4 », *in : Applied Algebra, Algebraic Algorithms and Error Correcting Codes*, 2001.

[35] A. Canteaut, P. Charpin, « Decomposing bent functions », *in : Workshop on Coding Theory and Data Integrity*, IMS, National University of Singapore, septembre 2001. Conférence invitée.

[36] A. Canteaut, É. Filiol, « Ciphertext only reconstruction of stream ciphers based on combination generators », *in : Proceedings of Fast Software Encryption (FSE 2000)*, *Lecture Notes in Computer Science*, 1978, Springer Verlag, New York, 2001.

[37] A. Canteaut, « Comment concevoir un chiffrement à clef secrète par blocs : exemple de l'AES », *in : Journée cryptographique de Limoges*, Limoges, décembre 2000.

[38] A. Canteaut, « Cryptographic Functions and Design Criteria for Block Ciphers », *in : Progress in Cryptology - INDOCRYPT 2001*, *Lecture Notes in Computer Science*, 2247, Springer-Verlag, p. 1–16, 2001. Conférence invitée.

[39] A. Canteaut, « Introduction à la cryptographie », *in : Séminaire X - Aristote - "Sécurité des transactions"*, octobre 2001.

[40] C. Carlet, P. Guillot, « Bent, resilient functions and the numerical normal form », *in : DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, *publié par l'AMS*, *56*, p. 87–96, 2001.

[41] C. Carlet, « On the complexity of cryptographic Boolean functions », *in : Sixth International Conference on Finite Fields and Applications*, Oaxaca, Mexique, Mai 2001. Conférence invitée.

[42] C. Carlet, « On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions », *in : Proceedings de SETA 2001 (Sequences and their Applications*, *Discrete Mathematics and Theoretical Computer Science*, Springer-Verlag, p. 131–144, Bergen, Norvège, mai 2001.

[43] N. Courtois, M. Finiasz, N. Sendrier, « How to achieve a McEliece-based Digital Signature Scheme », *in : Advances in Cryptology - Asiacrypt 2001*, *Lecture Notes in Computer Science*, 2248, Springer-Verlag, p. 157–174, 2001.

[44] E.M. Gabidulin, P. Loidreau, « Subfield subcodes of maximum-rank distance codes », *in : Proceedings of ACCT'7, (Juin 2000)*, p. 151–156, Bansko, Bulgarie, 2000.

[45] E. Filiol, C. Fontaine, D. Vianne, « A new, fast block cipher design : COS ciphers », *in : 2001 International Symposium On Information Theory*, IEEE Information Theory Society, p. 138, Washington D.C., USA, juin 2001.

[46] E. Filiol, C. Fontaine, « A New Ultrafast Stream Cipher Design : COS Ciphers », *in : 8th IMA Conference on Cryptography and Coding*, *Lecture Notes in Computer Science*, Institute for Mathematics and Applications, Springer-Verlag, Cirencester, Royaume-Uni, Dec. 17–20 2001. à paraître.

[47] É. Filiol, « Decimation attack of stream ciphers », *in : Proceedings of the First International Conference - INDOCRYPT'2000*, E. O. Bimal Roy (éditeur), *Lecture Notes in Computer Science*, *1977*, Indian Statistical Institute, Springer Verlag, p. 31–42, India, Calcutta, December 2000.

[48] G. Olocco, J.-P. Tillich, « A Family of Self-dual Codes which Behaves in Many Respects Like Random Linear Codes of Rate 1/ », *in : International Symposium on Information Theory*, 2001.

[49] F. Raynal, C. Fontaine, « About the links between cryptography and data hiding », *in : IS&T/SPIE International Symposium on Electronic Imaging 2002, Proceedings of the SPIE, 4675*, SPIE, 2001.

[50] N. Sendrier, G. Skersys, « On the Computation of the Automorphism Group of a Linear Code », *in : 2001 International Symposium On Information Theory*, IEEE Information Theory Society, Washington D.C., USA, juin 2001.

[51] N. Sendrier, « Practical and theoretical security of code-based public-key cryptosystems », *in : Workshop on Coding Theory and Data Integrity*, IMS, National University of Singapore, septembre 2001.

[52] C. Tavernier, « Construction of modular curves and computation of their cardinality on $\mathbb{F}_p$ », *in : Sixth International Conference on Finite Fields and Applications*, Oaxaca, Mexique, Mai 2001.

Rapports de recherche et publications internes

[53] N. Courtois, M. Finiasz, N. Sendrier, « How to achieve a McEliece-based Digital Signature Scheme », *rapport de recherche n°4118*, INRIA, Février 2001, `http://www.inria.fr/rrrt/rr-4118.html`.

Divers

[54] C. Aguilar, « Codes anti-collusion pour le fingerprinting », Mémoire de Stage, Ecole Polytechnique, 2001.

[55] M. Bardet-Turel, « Utilisation des bases de Groebner pour le décodage des codes cycliques », Mémoire de DEA Algorithmique, PARIS VI, 2001.

[56] A. Canteaut, P. Charpin, « Decomposing bent functions », soumis pour publication, 2001.

[57] A. Canteaut, E. Filiol, « On the Influence of the Filtering Function on the Performance of Fast Correlation Attacks on Filter Generators », soumis pour publication, 2001.

[58] A. Canteaut, M. Videau, « Higher order differential attacks on block ciphers using highly nonlinear confusion functions », soumis pour publication, 2001.

[59] A. Canteaut, « Approximations of nonlinear combining functions in stream ciphers », soumis pour publication, 2001.

[60] C. Carlet, C. Ding, « Highly Nonlinear Mappings », SIAM Journal on Discrete Mathematics, 2001, soumis pour publication.

[61] C. Carlet, A. Klapper, « Upper bounds on the numbers of resilient functions and of bent functions », soumis pour publication, 2001.

[62] C. Carlet, « On cryptographic complexity of Boolean functions », Finite Fields and Applications, 2001, soumis pour publication.

[63] F. Galand, « Codes $\mathbf{Z}_{2^k}$-linéaires, codes de Kerdock généralisés et construction de codes dont les paramètres dépassent ceux des meilleurs codes précédemment connus », Mémoire de DEA, Université de Caen, 2001.

[64] A. Lamouchi, « Fingerprinting, watermarking et video », Rapport de Stage, DUT Villetaneuse, 2001.

[65] C. Nedoloaia, « Sur un algorithme de calcul des polynômes des poids », Mémoire de DEA, Université de Limoges, 2001.

[66] G. Olocco, J.-P. Tillich, « A family of self-dual codes which behaves in Many Respect like random linear codes of rate 1/2 », 2001, soumis pour publication.

[67] N. Sendrier, A. Seznec, « HAVEGE : a User-level Software Unpredictable Random Number Generator », 2001, en préparation.

[68] C. Tavernier, « Construction of modular curves and computation of their cardinality on $\mathbb{F}_p$ », Finite Fields and Applications, 2001, soumis pour publication.

[69] M. Videau, « Généralisations de la cryptanalyse différentielle et critères de sécurité des chiffrements à clé secrète », Mémoire de stage de fin d'études, ENSICA, Toulouse, 2001.