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 **2**

2 Présentation et objectifs généraux **3**

3 Fondements scientifiques **4**

4 Résultats nouveaux **5**
4.1 Étude et analyse de structures discrètes 5
4.1.1 Groupes d'automorphismes 5
4.1.2 Codes équivalents. 6
4.1.3 Codes de Goppa 7
4.1.4 Codes cycliques et trinômes sur un corps fini 7
4.1.5 Théorie des nombres, algèbre finie 7
4.2 Cryptographie à clé publique 8
4.2.1 Système utilisant des codes correcteurs 8
4.2.2 Courbes elliptiques 9
4.3 Algorithmes de décodage et cryptanalyse 9
4.4 Primitives du chiffrement symétrique 11
4.5 Chiffrement symétrique: cryptanalyse 13
4.6 Protection des droits d'auteurs – watermarking 14

5 Contrats industriels (nationaux, européens et internationaux) **14**

6 Actions régionales, nationales et internationales **16**
6.1 Actions nationales 16
6.1.1 Contrats nationaux 16
6.1.2 Groupes de recherche 17
6.1.3 Participations à des instances et manifestations nationales 18
6.2 Actions internationales 18
6.2.1 Organisation de rencontres, expertises 18
6.2.2 Accueils de chercheurs étrangers 19

7 Diffusion de résultats **19**
7.1 Enseignement 19
7.2 Jurys de thèse 20
7.3 Participation à des colloques 21

8 Bibliographie **23**

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]

Conseiller scientifique

Guy Chassé [École des Mines de Nantes]

Collaborateurs extérieurs

Thierry Berger [Université Limoges]

Francis Blanchet [Lycée Montaigne]

Claude Carlet [Université Caen]

Caroline Fontaine [Université Lille]

Sami Harari [Université de Toulon]

François Laubie [Université Limoges]

Dominique Le Brigand [Université Paris 6]

Françoise Levy-dit-Vehel [ENSTA]

Ingénieurs experts

Hervé Alavoine [I.U.T. Villetaneuse, Université de Paris 13, de février à juillet 2000]

Nicolas Courtois [Université de Paris 6, de novembre à décembre 2000]

Doctorants

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

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

Matthieu Finiasz [ENS, depuis octobre 2000]

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

Gregory Olocco [Bourse MESR, co-direction avec Orsay, depuis septembre 1999]

Lancelot Pecquet [Bourse INRIA, depuis octobre 1997]

Cédric Tavernier [Bourse DGA, depuis septembre 2000]

Antoine Valembois [Bourse DGA, depuis septembre 1997]

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

Stagiaires

François Delost [Stage de DEA, Université de Limoges, d'avril à juin 2000]

Fatou Diop [Stage de fin d'Études, I.U.T. Villetaneuse, Université de Paris 13, d'avril à juin 2000]

Fabien Galand [Stage d'Été, Élève Ingénieur, ISMRA-ENSI de Caen, de juillet à août 2000]

Alexandre Hersans [Stage de DEA, Université de Paris Sud (XI), d'avril à août 2000]

Nicolas Israël [Stage de fin d'Études, ENSTA/COGENIT, de mars à septembre 2000]

Matthieu Lemoine [Stage de Maîtrise, ENSAE, de mai à juin 2000]

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 mèlent des travaux autant théoriques qu'appliqués utilisant tous les outils des mathématiques discrètes (algèbre des structures finies, combinatoire, géométries finies...) ainsi que ceux, plus modernes, de l'informatique théorique, notamment l'algorithmique et le calcul formel.

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

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

de recherche revêtant une grande importance pour les applications dans le domaine des télécommunications apparaissent qui justifient le développement d'une communauté possédant une palette large de compétences. Ceci apparaît dans les activités d'un nombre croissant de laboratoires de recherche dans le monde. Une étude récente de la NSF américaine[2]. – *Report of the Working Group on Cryptology and Coding Theory*, avril 1997. montre aussi la reconnaissance d'un nouveau domaine de recherche ainsi qu'une volonté institutionnelle de coordonner les efforts.

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

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

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 (T. Berger, [16, 71]) et un nouvel algorithme de preuve de l'équivalence de deux codes linéaires binaires (voir section suivante).

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

2. National Science Foundation

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 des codes de Goppa non cycliques dont le sous-code de poids pair est cyclique. Beaucoup parmi eux sont quasi-cycliques et ont des paramètres inconnus pour des codes quasi-cycliques. Certains atteignent les meilleures bornes connues pour des codes linéaires (voir [17, 15, 39]).

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

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

Cet algorithme, dit *algorithme de séparation du support (support splitting algorithm)* utilise les invariants du *Hull* – i.e. 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.

Un article décrivant cet algorithme dans un cadre plus général vient d'être accepté ; il s'agit d'un *regular paper* à IEEE-IT [35]. Les diverses applications possibles de l'algorithme, en relation avec la solidité de certains cryptosystèmes sont présentées dans §4.2.1.

Dans le cadre de sa thèse, G. Skersys a étudié avec N. Sendrier les algorithmes de calcul des groupes d'automorphisme des codes linéaires. Il a obtenu des améliorations importantes des algorithmes connus dans ce domaine. Plusieurs études sont en cours avec N. Sendrier.

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.

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 [33]. 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) [25, 52].

P. Loidreau a étudié les trinômes ternaires. Il a introduit des conditions d'existence de trinômes, sur le corps d'ordre 3, irréductibles et primitifs [70].

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 §4.4).

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 [59].

Ses travaux cette année ont porté d'une part sur les systèmes dynamiques nonarchimédiens (avec A. Salinier et A.Movahhedi [27]) et d'autre part sur les suites binaires minimalement auto-corrélées (avec M.Bauderon).

4.2 Cryptographie à clé publique

4.2.1 Système utilisant des codes correcteurs

Participants : Thierry Berger, Pierre Loidreau, Nicolas Sendrier.

Dans ce thème, sont regroupés 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). Une étude précise des invariants utilisés avait été réalisée par P. Loidreau pour son mémoire de DEA, et ceci aboutit à la mise en évidence de clés faibles dès que l'on veut cacher un ensemble de messages avec des codes de Goppa [32].

Cette année, P. Loidreau a étudié la possibilité de reduire 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'automorphisme. On peut ainsi développer des schémas cryptologiques plus résistants aux attaques connues. Ce travail a été présenté à ISIT 2000 et à ASIACRYPT [60, 61]. 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 [58].

P. Loidreau a dirigé le stage d'A. Hersans sur les algorithmes de décodage des codes MRD dans le langage de calcul formel MAGMA [76]. 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 [38].

4.2.2 Courbes elliptiques

Participant : Daniel Augot.

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

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

L'*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.

4.3 Algorithmes de décodage et cryptanalyse

Participants : Daniel Augot, Anne Canteaut, Gregory Olocco, Lancelot Pecquet, Michaël Trabbia, Antoine Valembois, Djessy Vianne.

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

L'étude des performances des *petits codes correcteurs en bloc* est d'actualité à cause du développement de systèmes où l'information est transmise *par paquets* de petites longueurs.

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

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 [78] ; ils ont proposé un algorithme itératif de décodage adapté à ces codes [63].

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. Un premier résultat, obtenu par D. Augot et L. Pecquet est un gain considérable sur la complexité de l'algorithme. Essentiellement, une méthode de factorisation à deux variables sur les corps finis est remplacée par une itération de Newton [14].

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 [64, 65].

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 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

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]

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 récemment conçu, avec M. Trabbia[8], 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. Ce travail a été présenté à Eurocrypt 2000 [44].

A. Valembois étudie, dans le cadre de sa thèse, les diverses procédures d'identification de codes linéaires. Le problème est, disposant d'un train binaire constitué de blocs de même longueur (les mots de code), de reconstituer le code utilisé. Le problème est d'autant plus simple que le canal est peu bruité [36]. Lorsque le bruit est important des techniques de décodage doivent être mise en oeuvre ; ceci a amené A. Valembois a proposer un nouvel algorithme de décodage souple [67]. A. Valembois a soutenu sa thèse en octobre [13].

4.4 Primitives du chiffrement symétrique

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

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

Les fonctions booléennes sont utilisées dans de nombreux systèmes de codage. 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*.

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 la non-linéarité maximum des fonctions booléennes, lorsque m est un nombre pair. Ce maximum est inconnu lorsque m est impair.

8. Stagiaire de l'École Polytechnique, avril à juin 1999.

La classification des fonctions courbes et la détermination de la non-linéarité en dimension impaire, sont des problèmes cruciaux, réputés très difficiles. La notion de diffusion[9] signifie, dans le cas du chiffrement par blocs par exemple, qu'une faible modification en entrée est diffusée dans l'ensemble du bloc de sortie. C'est un critère de fiabilité en cryptographie, dit *critère de propagation* pour les fonctions.

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 doivent permettre 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.

Les premiers résultats ont été présentés à ISIT 2000 et à EUROCRYPT 2000 [41, 40]. Un article long (50 pages) vient d'être accepté en tant que *regular paper* à la revue IEEE-IT [19]. P. Charpin a été invitée à deux *workshop* en Allemagne et aux USA [53, 54]. Des résultats spécifiques ont été obtenus par A. Canteaut sur les fonctions cubiques [23].

Fonctions courbes, presque courbes, presque parfaitement non-linéaires, et chiffrement à clés secrètes. C. Carlet poursuit un ensemble de travaux sur les fonctions courbes [51]. Il a obtenu avec Ph. Guillot, une caractérisation univoque des fonctions courbes binaires, la forme numérique normale (NNF). Celle-ci permet d'exprimer par des formules explicites le poids et le spectre de Fourier d'une fonction, de caractériser directement les fonctions courbes, de déduire de nouveaux invariants affines sur les fonctions booléennes et d'obtenir des propriétés de divisibilité des poids des fonctions. Ce travail a été présenté au colloque AAECC'13 [49].

La cryptanalyse linéaire et la cryptanalyse différentielle sont les principales attaques *connues* des systèmes de chiffrement à clé secrète. L'algorithme DES répondait à ces impératifs puisqu'aucune technique de cryptanalyse n'était sensiblement plus efficace que l'énumération de toutes les clefs possibles. Toutefois, comme sa clef secrète ne comportait que 56 bits, le DES était 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[10]. 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. Dans ce type de systèmes, 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.* C'est la permutation $x \longmapsto x^{-1}$ sur le corps d'ordre 256 qui a été choisie pour l'AES.

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

10. **AES Proposal: Rijndael**, Joan Daemen et Vincent Rijmen.
`http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`

Il est montré dans [5] que les fonctions presque courbes correspondent à des codes linéaires dont la distribution des poids est optimale. Dans le cas des fonctions puissances, ces codes sont en fait les duaux de certains codes cycliques à deux zéros. Grâce à cette analogie, A. Canteaut, P. Charpin et H. Dobbertin ont prouvé que les fonctions presque courbes sont entièrement caractérisées par la distance duale et la divisibilité des poids du code qui leur est associée. Ceci leur a notamment permis de démontrer une conjecture formulée par Welch en 1968, selon laquelle la fonction $x \mapsto x^{2^d}$, où $d = (m-1)/2 + 3$, est presque courbe sur $\mathbf{F}_{2^m}$ quand m est impair. Ce résultat est l'objet d'un *regular paper* dans *IEEE Transactions on Information Theory* [20] et a été présenté à *Fast Software Encryption 99*. Un article présentant l'ensemble des résultats obtenus est publié dans *Siam Journal of Discrete Mathematics* [21].

Fonctions équilibrées. Ce critère signifie qu'une fonction présente en sortie autant de "1" que de "0". É. Filiol étudie les propriétés combinatoires des fonctions booléennes équilibrées. Il s'agit, à partir de la forme algébrique normale d'une fonction booléenne, de détecter la classe de poids (sous-équilibrée, suréquilibrée ou équilibrée) à laquelle elle appartient. Les premiers résultats ont été publiés dans les actes de la conférence Cryptography and Coding [55].

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. Outre les résultats présentés à Eurocrypt, un résultat marquant a été obtenu par C. Carlet : utilisant la représentation de ces fonctions par leur NNF, il a déterminé la divisibilité globale maximale du spectre de Fourier des fonctions résilientes. Ce résultat a fait l'objet d'une note à l'Académie des Sciences de Paris [24].

4.5 Chiffrement symétrique: cryptanalyse

Participants : Anne Canteaut, Éric Filiol.

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, deux techniques ont été initiées par É. Filiol, puis mises en oeuvre et optimisées (ou en cours d'optimisation) 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). Les premiers résultats seront présentés par É. Filiol au colloque *Indocrypt* [56].

La deuxième attaque est en fait 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? É. Filiol a optimisé ses algorithmes avec A. Canteaut. Leurs travaux ont été présentés à *FSE 2000*, le principal colloque international de *chiffrement symétrique* (cf. [42] et une version longue dans [68]).

4.6 Protection des droits d'auteurs – watermarking

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

Le projet a participé, en 1995-98, au projet européen AQUARELLE qui avait pour objet d'homogénéiser les ressources culturelles actuellement existantes (tableaux, manuscrits, photographies ...). Les partenaires culturels ont demandé que soit mise en place une protection de ces images. La solution envisagée repose sur la technique du *filigrane, une "marque" invisible incrustée dans l'image, d'une manière secrète*. Si l'image est utilisée frauduleusement, l'ayant-droit peut attester qu'il est bien propriétaire de l'image. Ces travaux ont fait l'objet notamment d'un article *invité* à un numéro spécial IEEE [1] sur les techniques de marquage d'images qui reste une des références de notre projet.

Suite à ces travaux, un groupe de travail sur *les problèmes liés au copyright* en général a été installé sous la responsabilité (en 1999-2000) de M. Brunet[11]. 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 publié cette année un article de vulgarisation dans le journal *Pour la Science* [26]. Elle 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 [34]. 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.

5 Contrats industriels (nationaux, européens et internationaux)

Nous décrivons dans ce paragraphe nos activités de transfert scientifique et développement. Notre collaboration avec la société COGENIT ainsi que l'étude qui s'intitule *Analyse de trains binaires*, en partenariat avec Thomson-CSF et la DGA, se sont poursuivies cette année. Une étude pour le CCETT de Rennes portant sur les codes CORTEX (voir §4.3) a débuté fin 99 et se poursuivra en 2001. Enfin, ont été négociés cette année deux contrats, l'un sur le marquage des films et l'autre sur un protocole de commerce electronique.

11. Ingénieur du corps des télécommunications, affecté à l'INRIA
`http://www-rocq.inria.fr/codes/Watermarking`

Collaboration COGENIT-CODES : Réalisation d'un PCBL, 1997–99.
La réalisation de la bibliothèque logicielle cryptographique Scrhypp a été initiée par un financement ANVAR en 1997 et 1998. Le projet à été poursuivi en 1999 par le stage d'ingénieur CNAM de Christine Pourcelot puis par l'embauche de Hervé Alavoine comme ingénieur expert, financé par un nouveau contrat avec COGENIT, pour le premier semestre 2000. La bibliothèque est en voie d'achèvement et pourra être utilisée pour le projet iFIC (dans le cadre de PRIAMM) auquel le projet CODES participe. Le responsable de cette action, pour CODES, est N. Sendrier.

Collaboration CNET/INRIA+LACO : Etude 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.

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 nécéssite la conception d'un système de chiffrement spécifique (à très haut débit), ainsi que d'un système de marquage d'image 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).

PME "CÔTE BASQUE INFORMATIQUE", 2000.
Des chercheurs de CODES et du LACO, ont réalisé l'expertise d'un *protocole d'authentification et de signature par le biais d'un système informatique*. C'est A. Canteaut qui est responsable de cette action pour le projet Codes.

Le développement du commerce électronique reste conditionné par les possibilités de paiement sécurisé sur Internet. Consciente de ce problème, la société Côte Basque Informatique propose d'offrir aux internautes et commerçants affiliés un moyen de paiement électronique sécurisé. Le principe est que les internautes peuvent se référencer gratuitement ; ils se verront alors attribuer un mot de passe et un CD-ROM, qui leur permettront d'accéder à leur porte-monnaie électronique. L'objet de ce contrat, impliquant également le LACO (Laboratoire d'arithmétique, de calcul formel et d'optimisation, Université de Limoges), est de concevoir un protocole d'authentification et de signature permettant de garantir la sécurité de ce moyen de paiement (identification, intégrité des transactions...).

6 Actions régionales, nationales et internationales

6.1 Actions nationales

Collaboration scientifique et échanges se sont poursuivis en 2000, 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, Toulon 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

– Un contrat a été établi en 98 entre l'INRIA et les Écoles de Coëtquidan pour une durée de trois ans. Les partenaires sont respectivement le projet Codes et le Centre de Recherche des Écoles de Coëtquidan (CREC), nouvellement créé. P. Charpin est chargée de superviser les activités scientifiques de l'équipe *Mathématiques appliquées à la sécurité des systèmes d'information* et d'établir un ensemble d'interactions entre ce groupe et Codes. Des stagiaires sont accueillis chaque année; É. Filiol et D. Vianne, enseignants aux Écoles de Coëtquidan sont aussi chercheurs doctorants au projet. C'est dans le cadre de ce partenariat que nous organisons le colloque international *Workshop on Coding and Cryptography* (janvier 99 et janvier 2001).

– **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), et l'Université de Limoges (Y. Duursma). Le thème de recherche est celui de l'étude des courbes algébriques et leur utilisation pour la cryptographie [12].

– **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.

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).
Résumé. 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.

6.1.2 Groupes de recherche

Le projet participe à deux groupements de recherche nationaux :

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

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

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

L'intérêt de ces groupes de travail, qui ont fait l'objet d'un appel d'offre, est de regrouper la communauté nationale des chercheurs relevant d'un même thème scientifique.

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 [13] depuis Octobre 99.

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

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

12. `http://www-rocq.inria.fr/codes/Daniel.Augot/courbes/une.html`
13. `http://www-rocq.inria.fr/codes/Pierre.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, 27ème section (cnu) : C. Carlet.
- Université de Limoges, 25ème section (cnu) : T. Berger, P. Charpin, F. Laubie, D. Le Brigand.
- Université du Var, 27ème section (cnu) : C. Carlet, P. Charpin, S. Harari.
- Université de Marseille-Luminy, 27ème section (cnu) : S. Harari.
- Université Paris 6, 25ème section (cnu) : D. Le Brigand.
- INRIA-Rocquencourt, section d'audition du jury CR2 2000 : P. Charpin.

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

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

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.

A. Canteaut a participé à la table ronde *Ordinateurs de demain* dans le cadre du Temps des Sciences à Saint-Michel-sur-Orge, janvier 2000.

D. Augot, A. Canteaut et F. Morain ont fait un exposé de formation à la cryptographie dans le cadre du groupe de travail de l'OSSIR. L'OSSIR (Observatoire de la Securité des Systèmes d'Information et des Réseaux) est une association qui regroupe des utilisateurs travaillant sur la sécurité des systèmes.

Conférence Internationale sur les Mathématiques dans l'Industrie et les Services. Cette manifestation est organisée par l'École polytechnique dans le cadre de l'Année Mondiale des Mathématiques en association et sous le haut patronage de la SMF (Société Mathématique de France) et de la SMAI (Société de Mathématiques Appliquées et Industrielles). N. Sendrier a organisé, à la demande des organisateurs, une session de témoignage sur la cryptographie. Un autre chercheur du projet CODES, A. Canteaut, a donné une conférence au cours de cette session.

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* et *IEEE symposium on Information Theory* (ISIT).

Organisation de rencontres internationales :

- P. Charpin est membre du comité de programme de *IEEE Symposium on Information Theory* (ISIT2000), qui a eu lieu a Sorrente, Italie, en Juin 2000.
- 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.
- Les membres du projet préparent actuellement le colloque international `\emWorkshoponCodingandCryptogra` qui aura lieu en Janvier 2001 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, Éditeurs associés: P. Charpin (INRIA-Rocquencourt), M. Girault (SEPT, Caen), G. Kabatiansky (IPPI, Moscou), H. VanTilborg (Eindhoven).

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

6.2.2 Accueils de chercheurs étrangers

Le projet a une politique d'invitation "large", au plan national et au plan international. Le projet a accueilli, pour de courtes durées, en 2000 :

- Alexander Barg (Bell Laboratories, USA) ;
- Andreas Enge (Université de Augsburg, Allemagne) ;
- Jose Ignacio Farran Martin (Université de Valladolid, Espagne) ;
- Ernst Gabidulin (Institut de Physique et de Technologies, Moscou, Russie) ;
- Gintaras Skersys (Université de Vilnius, Lituanie) ;
- Victor Zinoviev (IPPI, Académie des Sciences de Moscou, Russie).

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 thé-

sards 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 license informatique de Paris VI. Renaud Rioboo et Thérèse Hardin ont défini le projet FOC[14], dont le but est de construire un système de calcul formel expérimental, en utilisant les connaissances acquises en sémantique des languages 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.

- Cours de langage C, cours sur les réseaux, A. Canteaut, DEA, DESS, Limoges.

- TPs de cryptographie, P. Loidreau à l'ENSTA.

- TP-TD Math-Info, L. Pecquet, Université de Paris 7.

- N. Sendrier est chargé de TP à l'École polytechnique, (tronc commun Informatique) depuis octobre 00.

7.2 Jurys de thèse

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

Janvier 00 I. Duursma,
Arithmétique des codes linéaires et des courbes algébriques,
Habilitation à diriger des Recherches, Marseille.
Jury : T. Berger.

Mars 00 N. Lagorce,
Une approche p-adique des codes convolutifs,
Thèse d'Université de Limoges.
Jury : T. Berger (direction), C. Carlet.

Septembre 00 F. Boudot,
Preuves d'égalité, d'appartenance à un intervalle et leurs applications,
Thèse d'Université de Caen.
Jury : T. Berger (rapporteur), C. Carlet.

14. `http://calfor.lip6.fr/~foc`

Octobre 00 A. Valembois,
Décodage, détection et reconnaissance des codes linéaires binaires,
Thèse d'Université de Limoges.
Jury : T. Berger, P. Charpin, N. Sendrier (co-direction), S. Harari (rapporteur), F. Laubie (président).

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

Décembre 00 P. Gaudry,
Algorithmique des courbes hyperelliptiques et applications à la cryptographie,
École polytechnique.
Jury : P. Charpin

Décembre 00 L. Pecquet,
Construction et décodage des codes géométriques,
Thèse d'Université de Paris 6.
Jury : D. Augot, P. Charpin (co-direction).

7.3 Participation à des colloques

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

Séjours courts dans des universités et laboratoires en 2000 :

- D. Augot et L. Pecquet : Université de Valladolid, Espagne (invités par J. I. Farran Martin), janvier.

- C. Carlet : Université de Mexico, Méxique (invité par Horacio Tapia Recillas pour une série de conférences en cryptographie), avril.

- P. Charpin : Université de l'Illinois à Chicago, USA (séminaires organisés par Vera Pless), octobre.

Participations aux colloques fin 99 et en 2000 :

- *Seventh IMA International Conference on Cryptography and Coding*, Cirencester, UK, 20-22 décembre 1999.
  Conférencier : É. Filiol.

- *École Jeunes Chercheurs du GDR ALP en Algorithmique et Calcul Formel*, Caen, France, 27-31 mars 2000.
  Conférencière invitée : A. Canteaut
  Conférenciers : P. Loidreau, L. Pecquet.

- FSE - *Fast Software Encryption*, New York, USA, 10-12 avril 2000.
  Conférencier : É. Filiol.
- AES 3 - *Advanced Encryption Standard*, New York, USA, 13-14 avril 2000.
  Conférencier : É. Filiol.
- *Workshop on Coding Theory*, Oberwolfach, Allemagne, 30 avril au 6 mai 2000.
  Conférencière invitée : P. Charpin.
- *Eurocrypt'00*, Bruges, Belgique, 14-18 mai 2000.
  Conférenciers : A. Canteaut, C. Carlet, P. Charpin, C. Fontaine.
- ACCT-VII - *International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, Bulgarie, 18-24 juin 2000.
  Conférenciers : T. Berger, P. Charpin (invitée), A. Otmani, P. Loidreau.
- ISIT'00 - *IEEE International Symposium on Information Theory*, Sorrente, Italie, 25-30 juin 2000.
  Conférenciers : T. Berger, A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, P. Loidreau, A. Valembois.
  Participants : D. Augot, N. Sendrier.
- *3rd European Congress of Mathematics*, Barcelone, Espagne, 10-14 juillet 2000.
  Conférencier : L. Pecquet.
- *Euroconferences in Mathematics - Curves and Abelian Varieties over Finite Fields and their Applications*, Anogia, Crète, Grèce, 29 juillet au 4 août 2000.
  Conférencier : L. Pecquet.
- *2nd International Symposium on Turbo Codes & Related Topics*,
  Brest, France, octore 2000.
  Conférenciers : G. Olocco et J.-P. Tillich.
- *The 38th Annual Allerton Conference on Communication, Control and Computing*, Allerton, Illinois, USA, 4-6 octobre 2000.
  Conférencière invitée : P. Charpin.
- *Colloque Science des Réseaux*, Pékin, Chine, 16-20 octobre 2000.
  Conférencière invitée : A. Canteaut.
- ISITA'00 - *International Symposium on Information Theory and its Applications*, Honolulu, Hawaii, USA, 5-8 novembre 2000.
  Conférencier : É. Filiol.
- *Asiacrypt'00*, Kyoto, Japon, 3-7 décembre 2000.
  Conférenciers : N. Courtois, P. Loidreau.
  Participante : F. Levy-dit-Vehel.

– *Indocrypt'00*, Calcutta, Inde, 10-13 décembre 2000.
Conférencier : É. Filiol.

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] 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.

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

[7] 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.

[8] 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.

[9] 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.

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

Livres et monographies

[11] 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 (Eindhove), à paraître.

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

Thèses et habilitations à diriger des recherches

[13] A. Valembois, *Décodage, détection et reconnaissance des codes linéaires binaires*, thèse de doctorat, Université de Limoges, octobre 2000.

Articles et chapitres de livre

[14] D. Augot, L. Pecquet, « A lifting method to replace factorization in Sudan's algorithm », *IEEE Transactions on Information Theory*, 1999, à paraître.

[15] T. Berger, « Goppa and related codes invariant under a prescribed permutation », *IEEE Transactions on Information Theory*, 2000, à paraître.

[16] T. Berger, « Groupes d'automorphismes des codes de Reed-Muller projectifs et homogènes », *Comptes Rendus de l'Académie des Sciences de Paris*, 2000, à paraître.

[17] T. Berger, « On the cyclicity of Goppa codes, parity-check subcodes of Goppa codes and extended Goppa codes», *Finite Fields and their Applications*, 6, 2000, p. 255–281.

[18] F. Blanchet, G. Bommier, «Binary quasi-cyclic Goppa codes», *Designs Codes and Cryptography 20*, 2000, p. 107–124.

[19] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, «On cryptographic properties of the cosets of R(1,m)», *IEEE Transactions on Information Theory*, 2000, à paraître, Regular paper.

[20] 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, Regular paper.

[21] 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.

[22] A. Canteaut, «La cryptographie», *Techniques Avancées*, 2000, Numéro spécial sur "La sécurité des systèmes d'information", à paraître.

[23] A. Canteaut, « On the weight distributions of optimal cosets of the First-Order Reed-Muller Code», *IEEE Transactions on Information Theory*, 2000, à paraître.

[24] C. Carlet, « On the divisibility properties and nonlinearity of resilient functions », *Comptes Rendus de l'Académie des Sciences de Paris*, 2000, à paraître.

[25] 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*, 2000, à paraître.

[26] C. Fontaine, « Tatouage des images numériques et protection des droits d'auteur », *Pour la Science*, 270, avril 2000, p. 102–106.

[27] F. Laubie, A. Movahhedi, A. Salinier, «Systèmes dynamiques non archimédiens et corps de normes», *Comp. Math.*, 2000, à paraître.

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

[29] F. Laubie, « Ramification de certaines extensions de Lie p-adiques », *Manuscripta Math. 100*, 1999, p. 197–202.

[30] F. Laubie, « A recursive definition of p-ary addition without carry », *Journal de théorie des nombres de Bordeaux 11*, 1999, p. 307–315.

[31] F. Laubie, « Substitutions commutatives de séries formelles », *Journal de théorie des nombres de Bordeaux*, 2000, à paraître.

[32] P. Loidreau, N. Sendrier, « Weak keys in McEliece public-key cryptosystem », *IEEE Transactions on Information Theory*, 2000, à paraître.

[33] P. Loidreau, « Codes derived from binary Goppa codes », *Problemy Peredachi Informatsii*, 2000, à paraître.

[34] F. 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, IS&T/SPIE International Symposium on Electronic Imaging 2001: Security and Watermarking of Multimedia Contents III, à paraître.

[35] N. Sendrier, « Finding the permutation between equivalent codes: the support splitting algorithm », *IEEE Transactions on Information Theory 46*, 4, juillet 2000, p. 1193–1203.

[36] A. Valembois, « Detection and recognition of a binary linear code », *Discrete Applied Mathematics*, 1999, à paraître.

Communications à des congrès, colloques, etc.

[37] D. Augot, A. Canteaut, F. Morain, «Cryptosystèmes, algorithmes et longueur de clefs», *in : Séminaire de l'OSSIR (Observatoire de la Sécurité des Systèmes d'Information et des Réseaux)*, 2000.

[38] T. Berger, P. Loidreau, « A Niederreiter version of the GPT public-key cryptosystem », *in : Proceedings of ACCT'7, (Juin 2000)*, Bansko, Bulgarie, 2000.

[39] T. Berger, « Quasi-cyclic Goppa codes », *in : Proceedings 2000 IEEE International Symposium on Information Theory*, IEEE, p. 195, Sorrente, Italie, juin 2000.

[40] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, «Fourier Spectrum of Optimal Boolean Functions via Kasami's Identities », *in : Proceedings 2000 IEEE International Symposium on Information Theory*, IEEE, p. 183, Sorrente, Italie, juin 2000.

[41] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, « Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions », *in : Advances in Cryptology - EUROCRYPT'2000*, B. Preneel (éditeur), *Lecture Notes in Computer Science*, 1807, p. 507–522, 2000.

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

[43] A. Canteaut, M. Trabbia, « Compared performance of fast correlation attacks on stream ciphers », *in : Proceedings 2000 IEEE International Symposium on Information Theory*, IEEE, p. 213, Sorrente, Italie, juin 2000.

[44] A. Canteaut, M. Trabbia, «Improved fast correlation attacks using parity-check equations of weight 4 and 5», *in : Advances in Cryptology - EUROCRYPT'2000*, B. Preneel (éditeur), *Lecture Notes in Computer Science*, 1807, p. 573–588, 2000.

[45] A. Canteaut, «Codes correcteurs et cryptographie à clef secrète (tutorial)», *in : École Jeunes Chercheurs Algorithmique et Calcul Formel du GDR ALP*, Caen, mars 2000.

[46] A. Canteaut, «Critères de conception des systèmes de chiffrement à clef secrète», *in : Conférence internationale sur les mathématiques dans l'industrie et les services*, École polytechnique, novembre 2000.

[47] A. Canteaut, « Design and analysis of secret-key ciphers », *in : Colloque inter-académique "Network Sciences" (Académie des Sciences - Chinese Academy of Sciences)*, Pékin, Chine, octobre 2000.

[48] C. Carlet, P. Guillot, « Bent, resilient functions and the numerical normal form », *in : Actes du DIMACS Workshop on Association Schemes, Novembre 1999*, Piscataway, USA, 1999. À paraître.

[49] C. Carlet, P. Guillot, «A representation of Boolean functions», *in : AAECC'13, Novembre 99*, *LNCS*, 1719, Springer-Verlag, p. 94–103, 1999.

[50] C. Carlet, «One-weight $\mathbf{Z}_4$-linear codes», *in : International conference on Coding Theory, Cryptography and Related Areas*, Buchmann, Hoholdt, Stichtenoth, Tapia-Recillas (éditeurs), Springer-Verlag, p. 57–72, 1999.

[51] C. Carlet, «Recent results on bent functions», *in : Proceedings on International Conference on Combinatorics, Information Theory and Statistics, Journal of Combinatorics, Information & System Sciences*, *24*, 3–4, p. 275–291, 1999.

[52] P. Charpin, A. Tietavainen, V. Zinoviev, «On binary cyclic codes with codewords of weight three and binary sequences with the trinomial property», *in : Proceedings of ACCT'7, (Juin 2000)*, Bansko, Bulgarie, 2000. Conférencière invitée.

[53] P. Charpin, «The derivatives of Boolean functions: some related problems in coding theory and cryptography», *in : 38th Annual Allerton Conference on Communication, Control, Computing*, Allerton house, Conference Center of the University of Illinois, octobre 2000. Conférencière invitée.

[54] P. Charpin, «On the classification of the cosets of the Reed-Muller code of order one», *in : Meeting: Coding Theory*, Institut Mathématique d'Oberwolfach, Allemagne, mai 2000. Conférencière invitée.

[55] É. Filiol, « Designs, intersecting families and weight of boolean functions », *in : 7th IMA Conference on Cryptography and Coding, Décembre 99*, *LNCS*, 1746, Springer-Verlag, p. 70–81, 1999.

[56] É. Filiol, «Decimation attack of stream ciphers», *in : Proceedings of the First International Conference - INDOCRYPT'2000*, Springer Verlag, India, 2000.

[57] É. Filiol, «Reconstruction of punctured convolutional encoders», *in : International Symposium on Information Theory and Applications*, Hawaii, novembre 2000.

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

[59] F. Laubie, « Systèmes dynamiques sur les entiers p-adiques », *in : Colloque en l'honneur de Jacques Martinet*, Université de Bordeaux 1, décembre 1999.

[60] P. Loidreau, « Large weight patterns decoding in Goppa codes and application to cryptography», *in : Proceedings 2000 IEEE International Symposium on Information Theory*, IEEE, p. 186, Sorrente, Italie, juin 2000.

[61] P. Loidreau, «Strengthening McEliece public-key cryptosystem», *in : Advances in Cryptology - ASIACRYPT 2000*, IACR, Springer-Verlag, décembre 2000.

[62] P. Loidreau, «Système GPT : actualité et perspectives», *in : École Jeunes Chercheurs Algorithmique et Calcul Formel du GDR ALP*, Caen, mars 2000.

[63] G. Olocco, J.-P. Tillich, « Iterative decoding of a new family of block turbo-codes», *in : Proceedings on 2nd International Symposium on Turbo Codes and Related Topics*, p. 303–306, Brest, France, 2000.

[64] L. Pecquet, « Algebraic-geometric codes in real life», *in : Curves And Abelian Varieties Over Finite Fields And Their Application*, Anogia, Crete, Greece, août 2000.

[65] L. Pecquet, « Building algebraic-geometric codes in MAGMA», *in : Third European Congress of Mathematics*, Barcelona, Espagne, juillet 2000. Collaboration avec Paweł Wocjan.

[66] L. Pecquet, « Construction des codes géométriques de Goppa», *in : École Jeunes Chercheurs Algorithmique et Calcul Formel du GDR ALP*, Caen, mars 2000.

[67] A. Valembois, «Fast soft-decision decoding of linear codes, stochastic resonance in algorithms», *in : Proceedings 2000 IEEE International Symposium on Information Theory*, IEEE, p. 91, Sorrente, Italie, juin 2000.

Rapports de recherche et publications internes

[68] A. Canteaut, É. Filiol, « Ciphertext only reconstruction of stream ciphers based on combination generators», *rapport de recherche n° RR-3887*, INRIA, Février 2000, `http://www.inria.fr/rrrt/rr-3887.html`.

[69] M. Lemoine, N. Sendrier, « Génération d'aléa à l'aide de l'indétermination du compteur de cycle d'un processeur», *rapport de recherche*, INRIA, 2000, En préparation.

[70] P. Loidreau, «On the factorization of trinomials over $GF(3)$», *rapport de recherche n° RR-3918*, INRIA, Avril 2000, `http://www.inria.fr/rrrt/rr-3918.html`.

Divers

[71] T. Berger, « Automorphism groups of homogeneous and projective Reed-Muller codes», 2000, soumis pour publication.

[72] A. Canteaut, F. Arnault, P. Gaborit, « Expertise d'un protocole d'authentification et de signature par le biais d'un système informatique », Rapport du contrat COTE BASQUE INFORMATIQUE, 2000.

[73] F. Delost, «Modèle de sécurisation de films sur Internet», Mémoire de stage de DEA, Université de Limoges, 2000.

[74] F. Diop, « Conception d'une interface pour un logiciel calculant la distance minimale d'un code correcteur», Mémoire de stage de DUT "Informatique et Génie informatique" (IUT de Villetaneuse, Université Paris Nord XIII), 2000.

[75] F. Galand, « Sur un problème ouvert en théorie des codes correcteurs d'erreurs », Mémoire de stage d'été, ISMRA-ENSI Caen, 2000.

[76] A. Hersans, « Étude et Implémentation des attaques de Gibson contre le cryptosystème », Mémoire de stage de DEA, Université de Paris VI, 2000.

[77] N. Israël, « Étude de générateurs d'aléa – Mise en place d'une librairie OpenPGP », Mémoire de stage de DEA Algorithmique, ENSTA, 2000.

[78] G. Olocco, J.-P. Tillich, « A family of self-dual codes which behaves like random linear codes of rate 1/2», 2000, soumis pour publication.