INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Codes

Codage et cryptographie

Rocquencourt

THEME SYM

Table of contents

1. Team

Responsable scientifique
Nicolas Sendrier [DR, INRIA]

Responsable permanent
Daniel Augot [CR, INRIA]

Assistante de projet
Christelle Guiziou-Cloitre [AJT]

Personnel INRIA
Pascale Charpin [DR]
Anne Canteaut [CR]
Jean-Pierre Tillich [CR]

Conseiller scientifique
Guy Chassé [École des Mines de Nantes]

Collaborateurs extérieurs
Thierry Berger [Université Limoges]
Claude Carlet [Université Paris 8]
Éric Filiol [ESAT]
Philippe Gaborit [Université Limoges]
Françoise Levy-dit-Vehel [ENSTA]
Pierre Loidreau [ENSTA]

Post-doctorants
Avishek Adhikari
Emmanuel Cadic
Marine Minier

Doctorants
Magali Bardet-Turel [AMN]
Raghav Bhaskar [Bourse Égide]
Thomas Camara [Bourse MESR]
Mathieu Cluzeau [Bourse DGA]
Frédéric Didier [Normalien]
Cédric Faure [Normalien]
Matthieu Finiasz [AMN]
Fabien Galand [Bourse BDI]
Yann Laigle-Chapuy [AMN]
Cédric Lauradoux [Bourse INRIA]
Carmen Nedeloaia [Bourse régionale]
Harold Ollivier [X-Telecom]
Ludovic Perret [Bourse MESR]
Emmanuel Prouff [ATER ENSIB]
Bassem Sakkour [Bourse syrienne]
Marion Videau [Bourse DGA]

Stagiaires
Cédric Faure [Stage de DEA, ENS Ulm, de mars à septembre 2004]
Yann Laigle-Chapuy [Stage de DEA, ENS Cachan, de mars à juillet 2004]
Stéphane Manuel [Stage de Maîtrise, Université de Paris 8, de juillet 2004 à mars 2005]
Andrea Roeck [Stage de Mastère, Université de Salzburg, octobre 2004]
Maxime Saintes [Stage de l'ENST, juillet 2004]

Racem Triki [Stage de DEA, ENSTA, de mars 2004 à septembre 2004]
Camille Vacher [Stage de DEUG, Université de Cergy-Pontoise, de juin à juillet 2004]

2. Overall Objectives

2.1. Présentation

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. Scientific Foundations

3.1. Fondements

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 fondés 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. New Results

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

Participant: Thierry Berger.

Reconnaître deux codes équivalents, reconnaître un code déstructuré par permutations, accélérer certaines procédures de décodage, tous ces problèmes relèvent de l'étude des automorphismes des codes – i.e. des transformations isométriques conservant le code. C'est un axe traditionnel du projet codes.

Cette année, T. Berger s'est intéressé aux codes fondés sur le métrique "rang", différente de la métrique de Hamming usuellement considérée. Pour cette métrique il a défini la notion d'isomorphisme et étudié les isométries de codes de Gabidulin et des codes hyperboliques. Il a caractérisé les groupes d'isométries et les groupes de permutations des codes de Gabidulin.

4.1.2. Codes cycliques et codes auto-duaux

Participants: Carmen Nedeloaia, Pascale Charpin, Philippe Gaborit.

Philippe Gaborit a etudié des constructions pour des codes ADN qui peuvent s'utiliser pour faire des codes barres ou du "DNA computing" [30], notamment à partir de bons codes comme certains codes auto-duaux sur GF(4).

[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.

4.1.3. Duaux des codes BCH

Participant: Carmen Nedeloaia.

Carmen Nedeloaia a continué l'étude des duaux des codes BCH. La construction carrée modifiée des codes affines-invariantes prouvée par Berger et Béery a permis de trouver deux sous-codes de distances minimales petites, et donc d'en déduire des estimations des distances minimales pour les duaux des codes BCH. Ces résultats sont importants en longueur 512, cas dans lequel seules quelques distances minimales était connues auparavant. Ils ont été aussi vérifiés par l'algorithme Canteaut-Chabaud de recherche de mots de petits poids dans un code.

4.1.4. Codes de Goppa

Participant: Matthieu Finiasz.

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

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

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

4.1.5. Codes sur des anneaux

Participants: Fabien Galand, Claude Carlet.

Fabien Galand a étudié une classe de codes Z_{2^k}-linéaires (images, par l'application de Gray généralisée, de modules sur l'anneau des entiers modulo 2^k) : la généralisation des codes de Kerdock introduite par Carlet. Il a pu montrer qu'elle ne donne pas de nouveaux codes ayant de bons paramètres, au moins pour ce qui est des petites longueurs.

4.1.6. Recherche de mots de poids faible dans un code

Participant: Carmen Nedeloaia.

Un travail en commun avec Ph. Gaborit (Univ. de Limoges) et Alfred Wassermann (Université de Bayreuth-Allemagne) a été mené autour d'un algorithme de calcul de mots de poids donnés et de ses applications au calcul des polynômes des poids. Rappelons ici qu'il s'agit d'un problème NP-dur, et que toute avancée algorithmique dans ce domaine est la bienvenue, tant du point de vue algorithmique que théorique (application à l'étude des paramètres d'un code donné), mais aussi cryptographique où, par exemple, de tels algorithmes peuvent être utilisés en cryptanalyse.

L'algorithme étudié consiste en une optimisation d'une méthode utilisée par Zimmermann pour le calcul des distances minimales. La parallélisation des calculs et la généralisation aux codes non-binaires, dus a A. Wassermann, nous ont permis de calculer les polynômes des poids de tous les codes duadiques (donc aussi des codes résidus quadratiques) et quadratiques doublement-circulants, pour de longueurs ≤ 152 dans le cas binaire et ≤ 96 dans le cas ternaire.

4.1.7. Codes de Gabidulin.

Participants: Thierry Berger, Pierre Loidreau.

Thierry Berger a construit de nouveaux codes MDS (Maximum Distance Separable) pour la métrique de Hamming à partir d'une sorte de "concaténation" de codes de Gabidulin et de codes binaires optimaux. Il a aussi analysé les algorithmes de décodage utilisant cette construction.

Pierre Loidreau et E.M. Gabidulin ont travaillé sur la structure des sous-codes sur des sous-espaces de codes de Gabidulin. Ils ont montré que la borne générique sur les dimensions était atteinte et qu'il existait des transformations bijectives préservant le rang entre ces codes et des codes de Gabidulin de taille plus petite. Ce travail étend le travail réalisé en 2000 sur les sous-codes trace de codes de Gabidulin.

P. Loidreau a travaillé sur la relation entre le problème de reconstruction des polynômes linéaires et le décodage des codes de Gabidulin. Il a montré qu'on pouvait en dériver un autre algorithme de décodage en temps polynomial en s'inspirant de l'approche de Welch et de Berlekamp pour le décodage des codes de Reed–Solomon.

4.1.8. Séquences et CDMA

Participants: Enes Pasalic, Cédric Tavernier, Thierry Berger.

Cédric Tavernier, a étudié avec Enes Pasalic, les séquences Gold-like, qui sont des séquences à coefficients d'autocorrélation maximum, utilisées en communication (codes CDMA). De nouvelles classes ont été trouvées, et des classes de polynômes linéaires de permutation préservant l'ensemble de séquence Gold-like ont été déterminées.

Thierry Berger a utilisé des séquences multi-niveau dans le cadre de l'étalement de spectre par modulation de phase, et aussi des codes à très faible rendement (1/32 ème) pour améliorer le nombre d'utilisateurs d'un système de transmission de type CDMA. C'est un travail en commun avec L. Dubreuil, en liaison avec l'IRCOM (Limoges) et le CNES (Toulouse).

4.2. Cryptographie à clé publique

4.2.1. Système de chiffrement utilisant des codes correcteurs

Participants: Daniel Augot, Thierry Berger, Cédric Faure, 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.

Cédric Faure a effectué son DEA sur la transposition en métrique rang de l'algorithme de chiffrement à clé publique Augot-Finiasz fondé sur le problème de la reconstruction des polynômes. Rappelons que Matthieu Finiasz et Daniel Augot avaient inventé en 2003 un nouveau système de chiffrement à clé publique, fondé sur la difficulté de reconstruire un polynôme d'après ses valeurs "bruitées". Ce système présentait des clés plus courtes que le système de McEliece, mais les blocs de chiffrements étaient beaucoup plus longs. Ce système avait été présenté à la conférence Eurocrypt 2003. Il a été cassé par Jean-Sébastien Coron ; une réparation avait été proposée en collaboration avec Pierre Loidreau. Cette réparation avait à nouveau été cassée par Jean-Sébastien Coron.

L'idée sous-jacente au travail mené par Cédric Faure, est de fonder la sécurité d'un système de chiffrement à clé publique non plus sur la difficulté de reconstruire un polynôme, mais sur la difficulté de reconstruire un *polynôme linéaire*. Il propose notamment un nouvel algorithme de chiffrement à clé publique, qui est essentiellement une version en métrique rang du schéma Augot et Finiasz, pour lequel il montre que toutes les attaques de Jean-Sébastien Coron ne peuvent se transposer telles quelles.

4.2.2. Fonction de hachage fondée sur le problème du décodage

Participants: Daniel Augot, Matthieu Finiasz, Nicolas Sendrier.

Daniel Augot et Matthieu Finiasz ont introduit une nouvelle fonction de hachage cryptographique, suivant les principes de la cryptographie à clé publique. Ce genre de construction remonte à Merkle et Damgard, mais reste limitée à cause de la faible performance (en temps d'exécution) des primitives de la cryptographie à clé publique. Dans le cas présent la primitive introduite est le calcul du syndrome et le problème NP-dur associé.

Nicolas Sendrier a déterminé la fonction d'encodage pour préparer les données, fonction qui permet d'avoir une plus grande résistance aux attaques et aussi d'obtenir une meilleure rapidité. Au final, la fonction de hachage produite est rapide et "à sécurité prouvée". Ces travaux ont été soumis au colloque Eurocrypt 2004 qui se déroulera à Interlaken.

Une attaque a été produite par Coron et Joux, en utilisant une généralisation du paradoxe des anniversaires, due à Wagner. Une étude approfondie de cette attaque, menée en 2004, a montré que cette attaque est toujours de nature exponentielle, et qu'il suffit d'augmenter légérement la taille des paramètres pour retrouver le niveau de sécurité désiré.

4.2.3. Implantation de cryptosystèmes fondés sur les codes correcteurs

Participants: Matthieu Finiasz, Pierre Loidreau, Nicolas Sendrier.

Le système de signature présenté par des membres du projet CODES à ASIACRYPT 2001, permet d'obtenir les signatures les plus courtes connues à ce jour (80 bits). En revanche ce système est relativement lent car il nécessite, pour des paramètres offrant une sécurité suffisante, un temps de calcul important, de l'ordre de deux minutes, en software. Une action (intitulée OCAM) en collaboration avec le projet ARENAIRE et le LIRMM a été montée dans le cadre de l'ACI Sécurité Informatique pour effectuer, entre autre, une implantation FPGA de l'algorithme de signature. Les premières estimations permettent d'espérer un temps de calcul pour une signature de l'ordre de la fraction de seconde, ce qui rendrait le système utilisable.

Au-delà du seul système de signature le projet OCAM nous envisagera la mise en oeuvre matérielle d'autres algorithmes cryptographiques à clé publique (McEliece, Niederreiter, Gabidulin, ...) qui posent des problèmes similaires d'implantation matérielles : algèbre linéaire rapide, algorithme d'Euclide ou de Berlekamp-Massey, calcul des racines d'un polynôme, opérateurs arithmétiques sur des extensions de corps finis. Enfin les implantations performantes des extensions de corps finis, et en particulier du corps à deux éléments, font parties des objectifs de cette action.

4.2.4. Cryptosystèmes fondés sur des problèmes combinatoires

Participants: Françoise Levy-dit-Vehel, Ludovic Perret.

L'ACI ACCES s'est terminée en septembre. Nous poursuivons le travail commencé dans le cadre de cette ACI concernant l'investigation de méthodes de cryptanalyse de schémas cryptographiques à clef publique dite "multivariable". Dans ce contexte, il s'agit de retrouver des transformations inversibles linéaires et/ou affines entre deux systèmes de polynomes multivariés sur des corps finis (problème connu sous le nom d'"isomorphisme de polynômes"). Des algorithmes pour la résolution de ce problème ont été proposés par Ludovic Perret, et communiqués à la conférence ISIT'04 en Juin à Chicago [67]. Depuis, d'autres méthodes ont été explorées pour trouver de nouvelles équations linéaires permettant de retrouver ces transformations. Ludovic Perret présentera ses résultats sur le sujet à la conférence ICPSS en Novembre [68]. Un article a également été soumis à la conférence Eurocrypt'05.

Un deuxième volet concerne les systèmes fondés sur des problèmes difficiles relevant de l'algorithmique des mots sur des monoïdes et groupes partiellement commutatifs. Les premiers résultats sur le sujet ont été présentés par Françoise Levy-dit-Vehel à la conférence YACC'04 à Porquerolles en Juin . Nous avons poursuivi cette étude par l'élaboration d'un algorithme permettant de cryptanalyser les instances particulières du problème des mots qui sont à la base de la construction du schéma de chiffrement de Abisha, Thomas et Subramanian (présenté a Indocrypt'03). Ce travail va être présenté à la conférence Indocrypt'04 en décembre. Nous explorons actuellement des méthodes de cryptanalyse d'autres schémas fondés sur des problèmes voisins.

4.2.5. Cryptosystèmes fondés sur des problèmes algébriques

Participants: Daniel Augot, Magali Bardet, Philippe Gaborit.

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

Une étude théorique a permis obtenir de nouveaux résultats sur la complexité du calcul de base de Gröbner pour des systèmes polynomiaux sur-déterminés. La notion de systèmes semi-réguliers est définie, et pour de tels systèmes les bornes de complexité existantes sont étendues (bornes de Macaulay : le degré maximal intervenant au cours d'un calcul de base de Gröbner). Cette borne détermine la taille d'une matrice, intervenant dans le calcul de la base de Gröbner, sur laquelle des opérations de réduction de ligne doivent être effectuées, et c'est cette opération qui a un coût dominant dans l'algorithme total de résolution. Ainsi est établie précisément la complexité du calcul de base de Gröbner. De tels systèmes apparaissent naturellement dans les problèmes provenant de la cryptographie (HFE). Ce travail est en collaboration avec J-C. Faugère (projet Spaces) et B. Salvy (projet Algo).

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

4.2.6. Signature par le "Extended Domain Hash"

Participant: Matthieu Finiasz.

Les preuves de sécurité de la plupart des systèmes de signatures actuels reposent sur une propriété idéale de la fonction de hachage utilisée, appelée Full Domain Hash (FDH). Pour prouver la sécurité du système de signature avec McEliece cette propriété n'est pas vérifiée. En revanche, on peut définir une propriété similaire appelée eXtended Domain Hash (XDH) qui permet aussi d'aboutir à une preuve de sécurité. Ce nouveau formalisme est exploitable dans ce cas précis, mais devrait certainement pouvoir s'appliquer à d'autres systèmes ou des problèmes similaires se posent. Il semble aussi qu'en se plaçant dans un contexte de XDH on puisse aussi se passer de l'étape de randomisation présente dans la plupart des systèmes, puisqu'il implique automatiquement une part d'aléa.

4.2.7. Sécurisation d'applications partagées

Participants: Daniel Augot, Raghav Bhaskar.

Raghav Bhaskar, étudiant de l'Indian Institute of Technology, a commencé une thèse sous la direction de V. Issarny et coencadrée par Daniel Augot. L'objectif de ce travail est de proposer des solutions cryptographiques aux problèmes de sécurité posés par les environnements distribués sans fil. En effet ces environnements (PDAs par exemple) sont très sujets aux attaques par écoute radio, il faut alors sécuriser les communications. Dans ce cadre, R. Bhaskar a étudié le scénario AdHocFS (partage de fichiers) du projet Arles, notamment les divers protocoles de mise en accord de clé multi-utilisateur (généralisations du protocole de Diffie-Hellman bien connu) permettant d'obtenir la sécurité demandée.

Ce travail part dans deux directions : l'implémentation des ces protocoles, et leur applicativité, l'autre part étant l'étude théorique des ces protocoles suivant la méthode de la sécurité prouvée.

Raghav Bhaskar a aussi trouvé une variante intéressante du protocole de Diffie-Hellman, biparti, qui se généralise bien au cas de n utilisateurs. Le protocole obtenu est plus performant que ceux qui existent déjà, tant au niveau du nombre de rondes de communication, qu'au niveau des quantités de données échangées. De plus une preuve formelle de sécurité a été établie, la sécurité de ce protocole reposant sur la difficulté du problème de Diffie-Hellman décisionnel.

Du point de l'implantation, Raghav travaille avec le projet Arles, et a progressivement fait évoluer l'implantation vers plus de rapidité.

Le projet CODES s'inscrit également parmi les projets ayant participé à l'initiative "Ad Hoc" de l'INRIA.

4.3. Algorithmes de décodage

Participants: Daniel Augot, Anne Canteaut, Frédéric Didier, Pierre Loidreau, Bassem Sakkour, Jean-Pierre Tillich, Magali Bardet-Turel.

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

l'apparition de nouvelles applications en correction d'erreurs et en cryptologie. La troisième est l'émergence de techniques de décodage dits itératifs, de bonne performance, mais difficiles à justifier théoriquement.

Un des axes de recherche est l'étude de familles de codes qui peuvent se décoder itérativement. Une des questions fondamentales qui se pose pour évaluer les performances d'une telle famille est de calculer la distance minimale (voire même tout le polynôme énumérateur de poids). Des résultats partiels ont été obtenus dans ce sens pour une classe très large de codes de Tanner. Jean-Pierre Tillich a notamment exhibé un critère très simple permettant d'assurer qu'une famille de codes de Tanner contienne une forte proportion de codes dont la distance minimale est linéaire en la longueur du code. Par ailleurs, il propose également une modification de la construction de Tanner, qui a pour propriété d'améliorer significativement le polynôme énumérateur des poids. L'intérêt de la modification est que le code de Tanner modifié peut être décodé aussi efficacement que le code de Tanner de départ, tout en ayant une courbe d'erreur après décodage itératif qui est significativement meilleure pour les forts rapports signal à bruit. Par ailleurs, cette amélioration peut aussi être appliquée à la famille des codes LDPC, et là aussi cela améliore significativement les performances du décodage itératif. Une partie de ces travaux a été publiée dans [70].

Le projet s'intéresse aussi au décodage des codes de Reed-Muller d'ordre faible, et ce principalement pour les liens entre ce problème et certaines cryptanalyses de systèmes de chiffrement. Ainsi, Bassem Sakkour et Pierre Loidreau ont travaillé sur l'algorithme de décodage des codes de Reed-Muller d'ordre 2 de Sidel'nikov et Pershakov. Ils en ont déduit une amélioration qui permet de décoder significativement plus loin sans augmenter la complexité du décodage. Les résultats sont pour l'instant expérimentaux.

Cédric Tavernier lui, essaye d'améliorer un algorithme du a Goldreich, Rubinfeld et Sudan qui permet de décoder ces mêmes codes. Cet algorithme ne fonctionne pas quand le corps est trop petit, notamment dans le cas binaire qui est le plus important en pratique. Cédric Tavernier essaye de mélanger cette approche avec celle de Dumer, qui construit un décodage récursif des codes de Reed-Muller. L'objectif est de pouvoir décoder au delà de la distance minimale. L'algorithme de Goldreich, Rubinfeld et Sudan a été complètement et précisément analysé, et C. Tavernier en a proposé une amélioration sensible, qui diminue concrètement le temps d'exécution le temps de décodage. Cet algorithme a été appliqué en cryptographie. Ces algorithmes ont été étendus aux codes de Reed et Muller d'ordre 2. L'analyse a été faite dans le cas du canal binaire symétrique (les erreurs sont uniformément réparties), et dans le cal du canal dit "adversaire", qui correspond en fait à faire l'analyse du pire cas.

Daniel Augot et Magali Bardet utilisent, pour le décodage dur des codes à résidus quadratiques (pour lesquels aucun algorithme de décodage général n'est connu), les bases de Groebner, en collaboration avec Jean-Charles Faugère. Des résultats sont obtenus pour des longueurs raisonnables, et aussi pour des codes cycliques jusque-là indécodables.

4.4. Reconnaissance de codes

Participants: Nicolas Sendrier, Mathieu Cluzeau, Anne Canteaut.

Ce travail de recherche fondamentale a été initié par une demande de la DGA. Il s'agit de retrouver sans connaissance préalable, à partir du résultat d'une écoute sur un canal radio, l'ensemble des techniques de codage utilisées par le système de communication observé (brasseur, code correcteur d'erreur,...). Il s'agit d'un travail fondamental mettant en œuvre diverses techniques de mathématiques discrètes, d'algèbre, de combinatoire et d'algorithmique.

4.5. Primitives du chiffrement symétrique

4.5.1. Fonctions booléennes

Participants: Anne Canteaut, Claude Carlet, Pascale Charpin, Philippe Gaborit, Emmanuel Prouff, 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 auto corrélées*. 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*.

Claude Carlet a poursuivi son étude de l'épaisseur algébrique et de la normalité des fonctions booléennes; il a obtenu de nouveaux résultats sur la nonlinéarité d'une classe de fonctions contenant les fonctions symétriques, ces résultats étant déduits de la normalité de ces fonctions [16]. Il a prolongé son étude de la nonlinéarité et de la résilience des fonctions de la classe de Maiorana-McFarland et de sa généralisation introduite à CRYPTO 2002, en l'étendant à l'étude du critère de propagation et en obtenant une nouvelle construction de fonctions courbes [14].

Il a introduit et étudié une construction de fonctions cryptographiques fondée sur la concaténation (selon le même principe que pour les fonctions de Maiorana-McFarland) des indicatrices d'espaces affines [15]. Il a également introduit et étudié une nouvelle construction secondaire de fonctions booléennes, qui généralise toutes les constructions secondaires connues [49]. En collaboration avec C. Ding, il a fait une étude approfondie des fonctions hautement non-linéaires définies et à valeurs dans les groupes abéliens [18]. En collaboration avec A. Klapper, il a introduit une nouvelle construction de séquences pour le CDMA [32]. En collaboration avec H. Dobbertin et G. Leander, il a introduit la notion d'extension normale de fonction courbe, qui a permis de montrer que la somme directe d'une fonction normale et d'une fonction non-normale est toujours non-normale [19]. En collaboration avec Emmanuel Prouff il a étudié les fonctions booléennes vectorielles en poursuivant l'étude des fonctions de Maiorana-McFarland, en généralisant la notion de séquence couvrante associée à de telles fonctions et en décrivant une attaque possible sur les boîtes S des schémas cryptographiques par blocs liée à ces séquences [52]. En collaboration avec W. Meier et E. Pasalic, il a formalisé et étudié la notion d'immunité algébrique des fonctions booléennes [65].

Claude Carlet et Philippe Gaborit ont récemment étudié une famille de fonctions contenues dans l'ensemble des fonctions courbes et possédant des propriétés encore plus spécifiques: les fonctions hyper-bent. Ils réussissent à donner des classifications de fonctions booléennes ayant jusqu'à 10 variables et montrent que dans de nombreux cas ces fonctions se réduisent aux fonctions PSap de Dillon. Ces résultats ont été présentés à la conférence ISIT 2004 à Chicago [51] et sont à paraître dans JCTA [20].

Anne Canteaut et Marion Videau se sont elles intéressées plus spécifiquement aux propriétés cryptographiques des fonctions booléennes symétriques. Rappelons qu'une fonction booléenne symétrique à n variables est caractérisée par le fait qu'elle peut être décrite par une table de vérité de taille $(n+1)$. Cette représentation courte est un argument majeur dans le choix de leur utilisation. Cependant, dans un contexte cryptographique, en vue d'une utilisation dans des systèmes de chiffrement ou des fonctions de hachage, il convient d'être vigilant aux propriétés cryptographiques de telles fonctions, d'autant qu'aucune fonction symétrique clairement adaptée à cette utilisation n'a pu être trouvée jusqu'alors. L'utilisation d'une propriété de périodicité d'une représentation des fonctions symétriques, a permis d'obtenir une nouvelle borne sur leur ordre de résilience. L'étude des dérivées de ces fonctions a également permis de déduire des propriétés concernant le critère de propagation. Ces résultats ont fait l'objet d'une publication lors de la conférence ISIT 2004 [71]. Une version longue de l'article incluant une étude détaillée des propriétés des fonctions symétriques de degré inférieur ou égal à 8, a permis d'obtenir la liste de toutes les fonctions symétriques équilibrées à n variables de degré inférieur à 8. L'article a été accepté pour publication à IEEE-IT [13].

Les travaux de Pascale Charpin se situent en amont et concernent:

I - Fonctions Booléennes:

– *La normalité des Fonctions Booléennes.* (voir [22]) L'objet de ce travail est d'abord une meilleure compréhension de la propriété de normalité dont l'intérêt est clair. Il s'agit, en effet, de déterminer, pour une fonction donnée, le plus grand espace affine sur lequel elle est constante. Ensuite, des résultats récents sur les

décomposition des fonctions sont utilisés pour proposer des améliorations des algorithmes de recherche de normalité.
– *Classification des fonctions Booéennes résilientes.* (voir [50][17]) Avec Claude Carlet, elle s'intéresse à la résilience qui est un critère de non-corrélations éxigé surtout dans les sytèmes de chiffrement par flot. Ce travail se place nettement en classification: les fonctions de degree 3 et de meilleur résilience sont complètement décrites, mais, comme attendu, ils montrent que leurs propriétés cryptographiques sont globalement mauvaises.
II - Fonctions Vectorielles:
– *Construction de fonctions vectorielles non linéaires et hautement résilientes.* (voir [23]) On construit ici des fonctions à n entrées et m sorties ayant de bonnes propriétés cryptographiques. Pascale Charpin et Enes Pasalic utilisent de petits codes projectifs et une méthode d'assemblage due a Johannesson et Pasalic. C'est l'aspect effectif de la construction qui est totalement nouveau.
II - Calcul de sommes exponentielles: Etude des spectres des fonctions de type $x \mapsto x^k$, i.e. le contexte est aussi bien l'étude de séquences, de fonctions booléennes ou de codes cycliques.
– *Exposants de Niho et codes à trois poids.* (voir [21]) Lorsque k est un exposant de Niho Pascale Charpin montre que la spectre associé ne peut avoir 3 valeurs.
– *Sommes de Kloosterman et codes BCH.* (voir [54]) C'est la fameuse fonction $x \mapsto x^{-1}$. De façon étonnante, la divisibilité du spectre est liée à la distribution des poids des cosets du BCh 3-correcteur.

4.6. Étude et conception de cryptosystèmes pour les réseaux de télécommunication

Participants: Daniel Augot, Anne Canteaut, Pascale Charpin, Jean-Pierre Tillich, Nicolas Sendrier, Matthieu Finiasz, Marion Videau, Marine Minier.

Le but du RNRT X-CRYPT est de construire un ensemble d'outils cryptographiques adaptés aux réseaux de télécommunications à haut débit. En particulier, les réseaux sans-fil provoquent des problématiques nouvelles en termes de sécurité, doivent faire face à de nouveaux types d'attaques et nécessitent la mise en place de mécanismes de sécurité adaptés. Quant aux solutions existantes, par exemple dans le domaine de chiffrement des communications, leur rapidité n'est souvent pas satisfaisante, notamment pour passer à des débits supérieurs, et leur sécurité peut sans aucun doute être améliorée. Un système de chiffrement satisfaisant aux critères de conception classiques peut très bien voir, par exemple, sa sécurité réduite par une nouvelle famille d'attaques cryptographiques. L'objectif du projet sera notamment, de disposer de systèmes avec davantage d'éléments de preuve de sécurité, pour résister également à des attaques qui seront proposées dans l'avenir.

4.7. Chiffrement symétrique : cryptanalyse

Participants: Anne Canteaut, Éric Filiol, Marion Videau, Daniel Augot, Cédric Tavernier, Marine Minier, Jean-Pierre Tillich.

4.7.1. Cryptanalyse des chiffrements par blocs

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

Toutefois, la résistance aux cryptanalyses linéaire et différentielle ne suffit évidemment pas à assurer la solidité d'un algorithme. Certains systèmes de chiffrement présentent ainsi des faiblesses particulières qui les rendent vulnérables à d'autres types d'attaques. Dans ce contexte, Anne Canteaut et Marion Videau se sont

récemment intéressées aux critères de résistance liés à la cryptanalyse différentielle d'ordre supérieur. Cette attaque, introduite par Lai et Knudsen en 1994, exploite l'existence d'un biais statistique dans la distribution des dérivées d'ordre supérieur de la fonction itérée. Elle s'applique notamment lorsque le degré multivarié de la fonction de chiffrement est petit. Mais, la détermination de ce degré est un problème difficile dans la pratique puisqu'elle nécessite une étude précise de l'évolution du degré au cours des itérations successives de la fonction de tour. C'est pourquoi le champ d'application de cette attaque était jusqu'à présent réduit aux systèmes utilisant une fonction itérée de petit degré. Anne Canteaut et Marion Videau ont alors montré que le degré de deux itérations d'une fonction était étroitement lié à la divisibilité de ses coefficients de Fourier. Cette étude les a notamment conduit à exhiber une attaque différentielle d'ordre supérieur très générale sur les chiffrements de Feistel utilisant une fonction itérée de non-linéarité optimale. Elle leur a également permis de comprendre l'origine d'une attaque sur l'algorithme MISTY1, dont une variante est utilisée pour assurer la confidentialité des communications pour les mobiles de troisième génération. Ces travaux ont montré que, paradoxalement, la vulnérabilité de MISTY1 aux attaques différentielles d'ordre supérieur résultait directement de l'utilisation de fonctions presque courbes, alors que celles-ci garantissent une résistance optimale aux attaques différentielles et linéaires. Cette étude a conduit à formuler un nouveau critère de sécurité pour les chiffrements itératifs par blocs impliquant le spectre de Fourier de la fonction itérée. Il apparaît alors que la fonction inverse dans un corps fini d'ordre 2^{2n}, qui a été choisie pour l'AES, est la seule fonction connue qui assure simultanément une résistance optimale aux attaques différentielles et linéaires, et aux attaques différentielles d'ordre supérieur.

4.7.2. Décodage et cryptanalyse

4.7.2.1. Chiffrement par bloc

Cédric Tavernier et Daniel Augot s'intéressent à l'approximation d'une fonction de chiffrement par une fonction plus simple, par exemple un polynôme de petit degré. Le point de départ de ces travaux est l'article de T. Jakobsen où il cryptanalyse l'algorithme de Knudsen et Nyberg, en utilisant l'algorithme de décodage de Sudan. Cette attaque semble difficile à généraliser pour d'autres fonctions de chiffrement (eg DES, AES...), et l'approche dite "univariée" a été abandonnée. Cédric Tavernier a utilisé les algorithmes de décodage des codes de Reed et Muller, introduits précédemment, pour trouver des approximations linéaires multivariées des sorties de versions réduites du DES.

De cette manière, il trouve de meilleures approximations que Matsui, dont les approximations sont celles de référence, sur des versions réduites du DES. Une expérience (lourde en calcul) à mener serait de conduire ces algorithmes de décodage sur une version complète du DES.

Cédric Tavernier a aussi étendu son algorithme de décodage aux codes de Reed et Muller *d'ordre deux*, ce qui revient à trouver des approximations quadratiques des sorties du DES. Les équations obtenues tiennent avec un bien meilleur biais que les équations linéaires. Reste maintenant à définir une cryptanalyse reposant sur ces équations quadratiques.

4.7.3. Cryptanalyse des chiffrements à flot

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

Anne Canteaut et Éric Filiol ont récemment amélioré les techniques classiques d'attaque par corrélation rapide dans le contexte des registres filtrés, c'est-à-dire des générateurs pseudo-aléatoires dont la sortie est

obtenue en appliquant une fonction booléenne à certaines cellules d'un registre à décalage à rétroaction linéaire. Dans ce contexte particulier, il est en effet possible de tirer partie de tous les coefficients de Fourier non nuls de la fonction de filtrage. Cette attaque est actuellement la cryptanalyse la plus efficace sur les registres filtrés. Une analyse précise a également permis de montrer que les performances de cette nouvelle attaque étaient pratiquement indépendantes des propriétés de la fonction de filtrage utilisée.

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

4.7.4. Attaques considérant la forme algébrique normale

L'attaque des systèmes de chiffrement symétriques, essentiellement fondée sur une approche combinatoire qui permet de trouver une information de nature plus qualitative que quantitative. L'angle privilégié par Eric Filiol est notamment de modéliser ces systèmes par un ensemble de fonctions booléennes et de trouver des structures biaisées dans leur forme algébrique normale (c'est-à-dire des polynômes multivariés où les bits de clef sont les variables). Ces structures peuvent alors être traduites de sorte à retrouver "facilement" des bits d'information sur la clef.

4.7.5. Testeurs

Cédric Tavernier a étudié les "testeurs" pour des programmes calculant des polynômes sur un corps fini. La construction des testeurs fait intervenir les codes de Reed-Solomon. Il faut donc réinterpréter les résultats théoriques en termes concrets, et dans le langage des codes correcteurs et de la cryptographie. On va supposer dans la suite que l'on travaille sur un corps fini du type F_{2^n} que l'on notera par commodité F_q. On dispose d'une boite noire que l'on peut modéliser comme une fonction $f : F_q \longrightarrow F_q$. Le testeur est un algorithme probabiliste, utilisant f comme oracle et devant répondre à la question "f est-elle proche d'un polynôme de bas degré".

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

Toutefois ces testeurs ont été appliqués au DES, sans succès, ce qui montre leur limite.

4.8. Génération logicielle de nombres aléatoires

4.8.1. Par l'entropie intrinsèque aux calculateurs

Participants: Nicolas Sendrier, André Seznec, Cédric Lauradoux.

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").

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. 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-aléatoires, ou par des procédé physiques externes à la machine.

Ce travail commencé en 2000 s'est tout d'abord déroulé dans le cadre de l'ARC Hipsor et a débouché sur le développement par André Seznec du logiciel HAVEGE (http://www.irisa.fr/caps/projects/hipsor/HAVEGE.html). Un article de fond décrivant l'ensemble des travaux à été publié dans le courant de l'année 2003 Depuis fin 2003 le travail se prolonge dans le cadre du projet de l'ACI Sécurité Informatique (projet UNIHAVEGE). En particulier, Cédric Lauradoux a commencé en novembre 2003 une thèse de doctorat sur la cryptanalyse d'HAVEGE.

4.8.2. Par les nombres 2-adiques

Participants: Thierry Berger, Abelkader Necer, François Arnault.

Les suites périodiques générés par des circuits 2-adiques ont été introduites précédemment par les participants sus-nommés. Ils ont, cette année, produit un algorithme de synthèse de ces suites périodiques (à la Berlekamp-Massey). Cet algorithme utilise l'algorithme d'Euclide étendu.

De plus ils ont conçus et analysé de nouveaux générateurs utilisant des circuits CSR filtrés.

4.8.2.1. Automates non linéaires

Il s'agit d'une étude plus théorique d'analyse de la sécurité des automates quadratiques ou hautement non-linéaires. En particulier, il s'agit d'étudier des attaques de type algébriques sur ces générateurs.

4.9. Protection des droits d'auteurs – watermarking

Participants: Françoise Levy-dit-Vehel, Nicolas Sendrier, Fabien Galand.

Fabien Galand a mené, avec G. Kabatiansky (IPIT, Russie) des travaux sur la dissimulation d'information (stéganographie), obtenant d'une part des bornes supérieures sur la capacité des schémas de dissimulation et d'autre part des schémas de dissimulation (l'ensemble étant fondé sur les codes de recouvrements). Dans le modèle sans adversaire actif, les schémas obtenus sont asymptotiquement optimales.

Françoise Levy-dit-Vehel participe au projet RNRT DIPHONET (DIffusion de PHOtographies à travers (I)nterNET - projet précompétitif, labellisé[3] concernant la protection des droits lors de la diffusion de photographies numériques à travers Internet) qui est en cours de finalisation. La partie cryptographique de ce projet consistait essentiellement à élaborer un protocole par lequel une entité est capable de prouver auprès d'autorités compétentes qu'une image I' trouvée sur Internet provient d'une image I qui lui appartient (le lien entre I' et I ayant au préalable été établi par des techniques de tatouage d'images). Ce protocole a été réalisé, et nous envisageons de déposer un brevet sur certains aspects du protocole (en collaboration avec le projet Temics de l'IRISA, et CANON).

4.10. Sécurité informatique et sécurité juridique

Participants: Anne Canteaut, Marion Videau.

[3] Projet pré-compétitif, labellisé en Mai 2001; participants : Canon, IRISA, Supelec (LSS).

Asphales est un projet de l'ACI Sécurité Informatique retenu en juin 2004 et initialisé en septembre 2004. Il regroupe les compétences de juristes et d'informaticiens afin d'étudier les interactions entre sécurité informatique et sécurité juridique. Isabelle de Lamberterie (CECOJI-CNRS) est la coordinatrice du projet qui regroupe en outre les équipes suivantes : CECOJI-CNRS, IREENATet Stic&Santé/IREENAT (université de Lille), LETUDIC/INT et LETUDIC/Télécom Bretagne, ERID (université de Montpellier), DANTE (université de Versailles Saint Quentin en Yvelines), CERDI (Paris XI) et CODES-INRIA.

4.11. Informatique quantique

Participants: Thomas Camara, Harold Ollivier, Jean-Pierre Tillich.

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

Les participants s'intéressent à la fiabilisation du calcul quantique et de la transmission d'information quantique à l'aide de codes correcteurs d'erreurs. Ce domaine n'a véritablement pris son essor qu'après 1997, année au cours de laquelle un formalisme efficace a permis l'exploration de vastes familles de codes quantiques. Les codes que nous avons commencé à développer sont les analogues quantiques des codes convolutifs. Harold Ollivier et Jean-Pierre Tillich ont développé un formalisme algébrique permettant de les étudier, et proposé un algorithme inspiré de l'algorithme de Vitterbi permettant de réaliser efficacement le décodage au maximum de vraisemblance. Par ailleurs dans le stage de Thomas Camara, un analogue quantique des codes à matrice de parité creuse (ou codes LDPC) a été introduit, et il a été montré que l'algorithme de décodage itératif classique se généralise au cadre quantique. L'objectif est maintenant de s'intéresser à la construction effective de codes à matrice de parité creuse quantiques, ainsi qu'à la construction d'analogues de turbo-codes quantiques.

5. Contracts and Grants with Industry

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

5.1.1. Collaboration France-Télécom RD-INRIA:

Étude de nouveaux turbo-codes en bloc, d'avril 2003 à décembre 2004. Le thème de ce contrat est de proposer des améliorations des turbo-codes classiques. Les responsables sont : Jean Pierre Tillich (INRIA) et Jean-Claude Carlach (France-Télécom-RD).

A ce titre, un post-doc Emmanuel Cadic a été recruté pour 2003-2004.

5.1.2. Contrat DGA-CELAR

Étude sur les applications des bases de Groebner en cryptologie, avec J.C. Faugère. Responsable : Anne Canteaut.

5.1.3. Contrat DGA

notifié en Juillet 2003, durée de un an. Le thème est d'essayer de reconnaître le code-correcteur utilisé sur une transmission, quand celui-ci est inconnu. Responsable : Nicolas Sendrier.

5.1.4. Banque de France

Daniel Augot, Jean-Pierre Tillich et Nicolas Sendrier ont fourni une étude pour la Banque de France, qui cherchait à mettre un authentifiant variable sur chaque billet. Cette étude précise notamment la méthode cryptographique la plus appropriée pour ce type de besoin. Il s'agit d'un pré contrat, devant éventuellement paver le chemin pour l'étude définitive.

6. Other Grants and Activities

6.1. Actions nationales

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

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

6.1.1. Contrats nationaux

6.1.1.1. CrAC – Action Concertée Incitative "Cryptologie" (2000-2003)

Titre: *CrAC – Cryptologie, Algorithmique et Codes* Coordinatrice du projet : P. Charpin.

Intervenants : D. Augot, A. Canteaut, C. Carlet, P. Charpin, N. Sendrier.

Le projet CODES a obtenu 91 KEuros sur trois ans du ministère de la recherche, dans le cadre d'une Action Concertée Incitative, *soutien aux équipes d'excellence*, pour soutenir sa recherche dans le domaine de la cryptographie.

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.

Le rapport final d'évaluation a été rendu en Juin 2003. Un prolongement pour 3 ans du financement de ce projet vient d'être obtenu dans le cadre de l'appel d'offres 2002 de l'Action Concertée Incitative "Cryptologie".

6.1.1.2. ACI Crac II

Le projet CRAC II s'inscrit dans le prolongement du projet CRAC présenté par les chercheurs du projet CODES et soutenu par l'ACI Cryptologie 2000. Son objectif est d'approfondir les travaux de l'équipe sur les systèmes à clef publique fondés sur les codes et sur la cryptographie symétrique, qui font l'objet de plusieurs thèses de doctorat débutées récemment au sein de CODES. Il a également pour but de renforcer les collaborations scientifiques initiées par le projet CRAC. Ce projet a obtenu un financement du Ministère de la Recherche de 75 KEuros sur une durée de trois ans à partir d'août 2002.

6.1.1.3. ACI PolyCrypt

Cette Action Concertée incitative se situe dans le cadre des échanges entre calcul formel et cryptologie. Elle est encadrée par Guillaume Hanrot, et les équipes Codes, Spaces (Loria et Rocquencourt) y participent. Tous les aspects algébriques de la cryptanalyse sont abordés dans cette ACI, notamment les attaques par bases de Gröebner.

6.1.1.4. ACI Réseaux quantiques

de septembre 2003 à août 2006, portant sur la fiabilisation de l'information quantique dans des réseaux quantiques. Ce projet est une collaboration entre le LRI et l'INRIA. Le responsable au niveau INRIA est Harold Ollivier.

6.1.1.5. ACI ACSION

de septembre 2004 à aoôut 2007, collaboration entre l'université Paris 8, Télécom Paris et l'INRIA, qui porte sur l'application de techniques de codes correcteurs d'erreurs en cryptologie. Le coordinateur de ce projet est Jean-Pierre Tillich.

6.1.1.6. ACI ASPHALES

de septembre 2004 à Août 2007, dont le sujet est l'étude des interactions entre sécurité informatique et sécurité juridique. Isabelle de Lamberterie (CECOJI-CNRS) est la coordinatrice du projet qui regroupe en outre les équipes suivantes : CECOJI-CNRS, IREENATet Stic&Santé/IREENAT (université de Lille), LETUDIC/INT et LETUDIC/Télécom Bretagne, ERID (université de Montpellier), DANTE (université de Versailles Saint Quentin en Yvelines), CERDI (Paris XI) et l'INRIA (projet CODES).

6.1.1.7. RNRTs

- RNRT X-CRYPT (avec Schlumberger, École normale supérieure, France Telecom, Cryptolog International, Université de Versailles) labellisé en 2003 (3 ans). Anne Canteaut est responsable du groupe "chiffrement à flot rapide".
- RNRT DIPHONET (DIffusion de PHOtographies à travers (I)nterNET - projet précompétitif. Responsable : Françoise Levy-dit-Véhel.

6.1.1.8. sixième PCRD européen

Réseau d'excellence européen ECRYPT. Anne Canteaut est responsable de la participation de l'INRIA, et du Working Group "Symmetric Cryptology: Strategic Research".

6.1.2. Groupes de recherche

Le projet participe à :

- GDR *Algorithmes Langages et Programmation* (AMI) : Claude Carlet a la responsabilité du groupe de travail intitulé *Codage et Cryptographie*.
- au GDR Information quantique (Harold Ollivier).
- groupe de travail *Archivage électronique* organisé par le Forum des Droits sur l'Internet et la Mission Economie Numérique (Anne Canteaut).

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[4] depuis octobre 99.

6.1.3. Participations à des instances et manifestations nationales

Plusieurs membres du projet participent à des commissions de spécialistes :
Université de Paris 8, 25e section (CNU) : C. Carlet, T. Berger, J P. Tillich.
Université de Limoges, 25e section (CNU) : T. Berger, A. Canteaut, C. Carlet, P. Charpin, P. Gaborit.
J.P. Tillich est membre de la commission de spécialistes de l'École Normale Supérieure 27e section. .
T. Berger est responsable de l'école doctorale de Mathématiques de l'université de Limoges, membre du bureau de l'école doctorale Science, Technologie, Santé de Limoges.
P. Charpin est membre membre du conseil de l'école doctorale de l'Université de Limoges, membre du comité scientifique de l'Action Concertée Incitative (ACI) "Cryptologie" (ministère de la recherche).
A. Canteaut est membre du comité scientifique d'Interstices, site Web de vulgarisation scientifique de l'INRIA.

6.2. Actions internationales

6.2.1. Organisation de rencontres

Le projet participe régulièrement à l'expertise des travaux de recherche pour les revues ou conférences internationales, notamment les revues *IEEE on Information Theory*, *IEEE on Computers*, *Designs Codes and*

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

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 :

- Daniel Augot est membre du comité de programme WCC2005 et a la responsabilité des soumissions electroniques à ce colloque.
- Anne Canteaut est membre des comités de programme de Crypto 2004, YACC 2004, FSE 2005, WCC2005 et préside le comité de programme d'Indocrypt 2004.
- Pascale Charpin est co-présidente du comité de programme de WCC2005.
- Françoise Lévy-dit-Véhel est membre du comité d'organisation de FSE 2005.
- Cédric Lauradoux est membre du comité d'organisation d'Indocrypt 2004.
- Nicolas Sendrier est membre du comité de programme WCC2005 et a organisé le colloque "ECRYPT Workshop on Provable Security", à Rocquencourt du 3 au 5 novembre 2004.
- Pierre Gaborit est organisateur des journées annuelles de Cryptographie et de Sécurité de l'information de Limoges (120 participants).
- Claude Carlet est membre du comité de programme de FSE 2004 et SETA 04.

Organisation de séminaires et de rencontres nationales :

- Pierre Loidreau organise le séminaire CCA (Codage, Codes et Algorithmique) qui se tient mensuellement à l'ENSTA.
- Nicolas Sendrier est l'organisateur du cycle "Les mathématiques du secret" dans le cadre des thématiques INRIA (3 conférences mai, juin, septembre 2004).
- Marine Minier est membre du comité de programme des journées C2 (Codage et Cryptographie) qui se tiendront du 30 janvier au 4 février 2005 à Aussois.

Revues :

- C. Carlet est Associate Editor pour la revue "IEEE Transactions on Information Theory" (spécialité "Coding Theory").
- P. Charpin est membre du comité d'édition de la revue internationale *Designs, Codes and Cryptography*, membre du conseil consultatif de l'encyclopédie de cryptologie intitulée *Encyclopedia of Information Security*, éditrice associée pour *IEEE Transactions on Computers*, dans la spécialité *codage*.
- C. Carlet est éditeur de la Special issue in Coding and Cryptography, dans la revue Discrete Applied Mathematics.

6.2.2. Accueils de chercheurs étrangers

- Hans Dobbertin, Université de Bochum, Allemagne ;
- Harald Niederreiter, National University of Singapore, Singapour ;
- Ernst Gabidulin, Institute of Physics and Technology, Dept. of Radio, Moscou, Russie ;
- Tor Helleseth, University of Bergen, Norvège ;
- Gregory Kabatiansky, IPIT, Moscou, Russie ;
- David Poulin, Institute for quantum computing, Canada ;
- Alexander Vardy, Université de San Diego, Etats-Unis ;
- Victor Zinoviev, IPIT, Moscou, Russie ;

7. Dissemination

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 mastères de Caen, Limoges et Toulon, nous sommes particulièrement impliqués dans le mastère parisien MPRI. Précisément, les enseignements ou cours de formation permanente cette année ont été:

- T. Berger est responsable de la formation doctorale de mathématiques de l'Université de Limoges.
- T. Berger est membre du bureau de l'école doctorale Science, Technologie, Santé de Limoges.
- Daniel Augot et Jean-Pierre Tillich interviennent dans le MPRI Algorithmique, filière Traitement et protection de l'Information, pour assurer un cours de codes correcteurs d'erreurs.
- A. Canteaut enseigne la *programmation en langage* C *pour la cryptographie* dans le Mastère Recherche de l'Université de Limoges et un cours de *logiciels cryptographiques* en Mastère professionel dans la même université.
- N. Sendrier est chargé d'enseignement à l'École Polytechnique au département d'informatique. Cours enseignés : Algorithmique et programmation (travaux dirigés), Introduction à la théorie de l'information (cours + TD).
- TPs de cryptographie, P. Loidreau à l'ENSTA.
- F. Levy-dit-Vehel enseigne un cours "Primitives cryptographiques" en troisième année à l'ENSTA, elle a aussi donné un exposé "Introduction à la cryptographie' à l'École thématique du CNRS VCARS.

7.2. Jurys de thèse

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

Janvier 2004 S. Leveiller, Thèse d'Université de l'ENST, *Quelques algorithmes de cryptanalyse du registre filtré*. Jury : A. Canteaut (rapporteur).

Mai 2004 M. Quisquater, Thèse d'Université de Louvain, Belgique, *Applications of character theory and the Möbius inversion principle to the study of cryptographic properties of Boolean functions*. Jury : C. Carlet.

Juin 2004 E. Prouff, Thèse d'Université de Caen, *Étude des fonctions booléennes et vectorielles pour la cryptographie*. Jury : C.. Carlet (directeur de thèse), A. Canteaut, T. Berger (rapporteur).

Septembre 2004 A. Gouget, Thèse d'Université de Caen, *Etude de propriétés cryptographiques des fonctions booléennes et algorithme de confusion pour le chiffrement symétrique*. Jury : C. Carlet (directeur de thèse).

Septembre 2004 C. Nègre, Thèse d'Université de Montpellier, *Opérateurs arithmétiques pour la cryptographie basée sur les courbes elliptiques*. Jury : N. Sendrier (rapporteur).

Octobre 2004 P. Rosendahl, Thèse d'Université de Turku, Finlande, *Niho Type Cross-Correlation Functions and Related Equations*. Jury : C. Carlet ("opponent").

Octobre 2004 M. Finiasz, Thèse d'Université de l'École Polytechnique, *Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clé publique*. Jury : T. Berger (rapporteur), N. Sendrier (directeur de thèse).

Décembre 2004 F. Galand, Thèse d'Université de Caen *Construction de codes Z_{p^k} linéaires de bonne distance minimale et schémas de dissimulation fondés sur les codes de recouvrement*. Jury : C. Carlet (directeur de thèse), T. Berger (rapporteur).

Décembre 2004 P. Gaborit, Habilitation à diriger des recherches, Université de Limoges, *Codes autoduaux et applications des codes*. Jury : C. Carlet (rapporteur), T. Berger.

Décembre 2004 M. Bardet, Thèse d'Université de Paris VI, *Étude de systèmes algébriques surdéterminés. Application aux codes correcteurs et à la cryptologie*. Jury :D. Augot (co-directeur de thèse).

Décembre 2004 G. Leander, *Normality of bent functions. Monomial- and Binomial-bent functions.* , Thèse d'Université de Bochum, Allemagne, . Jury : C. Carlet (rapporteur).

7.3. Participation à des colloques

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

Séjours courts dans des universités ou laboratoires en 2004 :

- Collaboration avec Los Alamos National Laboratory et l'université de Californie. Harold Ollivier a été invité d'avril à mai.
- Collaboration avec le Perimeter Institute Canada. Harold Ollivier a été invité de janvier à février.
- Collaboration avec l'Université de Bergen (Norvège), Marion Videau a été invité pendant 6 mois, et Pascale Charpin y a passé quelques semaines.
- Collaboration avec l'Université de St-Petersburg, Russie. Pascale Charpin a été invitée en avril 2004, dans le cadre du programme ECONET de collaboration Bulgarie-Russie-France (géré par P. Loidreau).

Participations aux colloques en 2004 :

- Seventh Workshop on Quantum Information Processing, 15 au 19 janvier 2004, Toronto, Canada, participant: H. Ollivier.
- FSE, 4 au 12 février 2004, Delhi, Inde, participant : C. Carlet.
- TCC, 19 au 21 février 2004, Washington, USA, participant : L. Perret.
- AES4, 10 au 12 mai 2004, Bonn, Allemagne, participants : D. Augot, A. Canteaut, M. Minier.
- EUROCRYPT, 9 au 12 mai 2004, Interlaken, Suisse, participant : C. Carlet.
- YACC, 1er au 5 juin 2004, Porquerolles, participants : A. Canteaut, C. Carlet, P. Loidreau.
- CRYPTARCHI, 16 au 19 juin 2004, Labussière sur Ouche, participant : C. Lauradoux.
- ACCT, 19 au 26 juin, Kranevo, Bulgarie, participants : P. Charpin, P. Loidreau, C. Tavernier.
- Fourth Canadian School, 21 au 25 juin 2004, Waterloo, Canada, participant : T. Camara.
- ISIT, 27 juin au 2 juillet 2004, Chicago, USA, participants : D. Augot, A. Canteaut, C. Carlet, M. Cluzeau, L. Perret, F. Lévy, N. Sendrier, J.-P. Tillich, M. Videau.
- CRYPTO, 15 au 19 aout 2004, Santa Barbara, USA, participants : A. Canteaut, C. Lauradoux, M. Minier.
- Fourth Conference on Security in Communication Networks, 7 au 12 septembre 2004, Amalfi, Italie, participant : R. Bhaskar.
- SACS,14-15 octobre 2004, Bruges, Belgique, participants : D. Augot, A. Canteaut, P. Charpin, M. Minier, J. P. Tillich.
- SETA, 24 AU 28 octobre 2004, Séoul, Corée, participant : C. Carlet.
- ACM CCS, 25 au 29 octobre 2004, Washington, USA, participant : R. Bhaskar.
- Journées ACI SI, 15 au 17 novembre 2004, Toulouse, partipants : D. Augot, P. Charpin, E. Filiol, C. Lauradoux, N. Sendrier, J.P. Tillich.
- INDOCRYPT, 20 au 22 décembre 2004, Chennai, Inde, participants : A. Canteaut, A. Enge, L. Perret, F. Lévy.

8. Bibliography

Books and Monographs

[1] P. CHARPIN, G. KABATIANSKY (editors). *Discrete Applied Mathematics - Special issue in Coding and Cryptology*, Éditeurs associés: A. Barg (U. of Maryland, USA), H. Gilbert (France Telecam R&D), T. Klove (Bergen, Norvège), J. Massey (U. of Lund, Suède), G. Zémor (ENST, Paris), to appear., Elsevier, 2004.

Doctoral dissertations and Habilitation theses

[2] M. BARDET. *Etude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.*, Thèse de doctorat, Université Paris 6, December 2004.

[3] M. FINIASZ. *Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clef publique*, Thèse de doctorat, Ècole Polytechnique, Palaiseau, October 2004.

[4] F. GALAND. *Constructions de codes Z_{p^k}-linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrements.*, Thèse de doctorat, Université de Caen, December 2004.

[5] H. OLLIVIER. *Elements de théorie de l'information quantique, décohérence et codes correcteurs d'erreurs.*, Thèse de doctorat, Ècole Polytechnique, Palaiseau, September 2004.

[6] C. TAVERNIER. *Testeurs, problèmes de reconstruction univariés et multivariés, et application à la cryptanalyse du DES.*, Thèse de doctorat, Ècole Polytechnique, Palaiseau, January 2004.

Articles in referred journals and book chapters

[7] F. ARNAULT, T. BERGER, A. NECER. *Feedback with Carry Shift Registers synthesis with the Euclidean Algorithm*, in "IEEE Trans. Inform. Theory", to appear, 2004.

[8] F. ARNAULT, T. BERGER, A. NECER. *Feedback with Carry Shift Registers synthesis with the Euclidean Algorithm*, in "IEEE Trans. Inform. Theory", vol. 50, n° 5, may 2004, p. 910-916.

[9] C. BACHOC, P. GABORIT. *Designs and self-dual codes with long shadows*, in "Jour. Comb. Theory Series A", vol. 1, n° 105, 2004, p. 15-34.

[10] T. P. BERGER, P. LOIDREAU. *How to mask the structure of codes for a cryptographic use*, in "Designs, Codes and Cryptography", to appear, 2004.

[11] S. BEZRUKOV, R. ELSASSER, B. MONIEN, R. PREISS, J. TILLICH. *New spectral lower bounds on the bisection width*, in "Theoretical Computer Science", vol. 320, 2004, p. 155-174.

[12] A. CANTEAUT, M. DAUM, G. LEANDER, H. DOBBERTIN. *Normal and Non Normal Bent Functions*, in "Discrete Applied Mathematics", to appear, 2004.

[13] A. CANTEAUT, M. VIDEAU. *Symmetric Boolean functions*, in "IEEE Trans. Inform. Theory", Regular paper, à paraitre, 2004.

[14] C. CARLET. *On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions highly nonlinear Mappings*, in "Journal of Complexity", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, "Complexity Issues in Cryptography and Coding Theory"., 2003, p. 182-204.

[15] C. CARLET. *Concatenating indicators of flats for designing cryptographic functions*, in "Designs, Codes and Cryptography", to appear, 2004.

[16] C. CARLET. *On the degree, nonlinearity, algebraic thickness and non-normality of Boolean functions, with developments on symmetric functions*, in "IEEE Transactions on Information Theory", vol. 50, 2004, p. 2178-2185.

[17] C. CARLET, P. CHARPIN. *Cubic Boolean functions with highest resiliency*, in "IEEE Trans. Inform. Theory", to appear, 2004.

[18] C. CARLET, C. DING. *Highly Nonlinear Mappings*, in "Journal of Complexity", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, "Complexity Issues in Cryptography and Coding Theory", vol. 20, n° 2-3, 2004, p. 205-244.

[19] C. CARLET, H. DOBBERTIN, G. LEANDER. *Normal Extensions of Bent Functions*, in "IEEE Transactions on Information Theory", to appear, 2004.

[20] C. CARLET, P. GABORIT. *Hyper-bent functions and cyclic codes*, in "Jour. Comb. Theory Series A", to appear, 2004.

[21] P. CHARPIN. *Cyclic codes with few weights and Niho exponents*, in "Jour. Comb. Theory Series A", vol. 108, n° 2, November 2004, p. 247-259.

[22] P. CHARPIN. *Normal Boolean functions*, in "Journal of Complexity", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, "Complexity Issues in Cryptography and Coding Theory", vol. 20, 2004, p. 245-265.

[23] P. CHARPIN, E. PASALIC. *Highly nonlinear resilient functions through disjoint codes in projective spaces*, in "Designs Codes and Cryptography", 2004.

[24] E. FILIOL. *Analyses de codes malveillants pour mobiles : le ver CABIR et le virus DUTS*, in "MISC - Le journal de la sécurité informatique", vol. 16, November 2004.

[25] E. FILIOL. *Le chiffrement par flot*, in "MISC - Le journal de la sécurité informatique", vol. 16, November 2004.

[26] E. FILIOL. *Le ver Blaster/Lovsan*, in "MISC - Le journal de la sécurité informatique", vol. 11, January 2004.

[27] E. FILIOL. *Le ver MyDoom*, in "MISC - Le journal de la sécurité informatique", vol. 13, mai 2004.

[28] J. FRIEDMAN, J. TILLICH. *Wave equations for graphs and the edge-based Laplacian*, in "Pacific Journal of Mathematics", vol. 216, n° 2, October 2004, p. 229-266.

[29] J. FRIEDMAN, J. TILLICH. *Generalized Alon-Boppana Theorems and Error-Correcting Codes*, in "SIMA Journal of Discrete Mathematics", to appear, 2005.

[30] P. GABORIT, O. D. KING. *Linear Constructions for DNA Codes*, in "Theoretical Comp. Science", to appear, 2004.

[31] P. GABORIT, C. S. NEDELOAIA, A. WASSERMANN. *Weight enumerators of duadic and quadratic residue codes*, in "IEEE Trans. Inf. Theory", to appear, 2004.

[32] A. KLAPPER, C. CARLET. *Spectral Methods for Cross-Correlations of Geometric Sequences*, in "IEEE Trans. Inform. Theory", vol. 50, 2004, p. 229-232.

[33] P. LOIDREAU. *Sur la reconstruction des polynômes linéaires : un nouvel algorithme de décodage des codes de Gabidulin*, in "Comptes Rendus de l'Académie des Sciences : Série I", 2004.

[34] C. S. NEDELOAIA. *Upper bounds on the dual distances of $EBCH(512, k)$ codes*, in "Designs, Codes and Cryptography", submitted, 2004.

[35] H. OLLIVIER, P. PAJOT. *La décohérence, espoir du calcul quantique*, in "La Recherche", vol. 378, n° 34, 2004.

[36] H. OLLIVIER, D. POULIN, W. H. ZUREK. *Environment as witness: selective proliferation of information and emergence of objectivity*, in "arXiv", vol. quant-ph, n° 0408125, 2004.

[37] H. OLLIVIER, D. POULIN, W. H. ZUREK. *Objective properties from subjective quantum states: Environment as a witness*, in "Phys. Rev. Lett.", to appear. Also arXiv, quant-ph 0307229 (2003), 2004.

[38] H. OLLIVIER, J.-P. TILLICH. *Quantum convolutional codes: fundamentals*, in "arXiv", vol. quant-ph, n° 0401134, 2005.

[39] G. OLOCCO, J. TILLICH. *A family of self-dual codes which behave in many respects like random linear codes of rate 1/2*, in "IEEE Trans. Inform. Theory", to appear, 2005.

[40] F. PETITCOLAS, C. FONTAINE. *Tatouage de documents audiovisuels numériques*, chap. Nouveaux outils pour l'évaluation des algorithmes de tatouage, Hermès-Lavoisier, 2004.

[41] D. POULIN, R. BLUME-KOHOUT, R. LAFLAMME, H. OLLIVIER. *Exponential speed-up with a single bit of quantum information: measuring the average fidelity decay*, in "Phys. Rev. Lett.", vol. 92, n° 17, 177906, 2004.

[42] N. SENDRIER. *Linear Codes with Complementary Duals Meet the Gilbert-Varshamov Bound*, in "Discrete Mathematics", vol. 285, 2004, p. 345-347.

[43] J. TILLICH, G. ZÉMOR. *The Gaussian isoperimetric inequality and decoding error probabilities for the Gaussian channel*, in "IEEE Transactions on Information Theory", vol. 50, n° 2, February 2004, p. 328-331.

Publications in Conferences and Workshops

[44] F. ARNAUD, T. BERGER. *Design of new pseudo-random generators based on a filtered FCSR automaton*, in "The State of the Art of Stream Ciphers, ECRYPT, Brugges, Belgium", October 2004.

[45] M. BARDET, J. FAUGÈRE, B. SALVY. *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations*, in "Proc. ICPSS International Conference on Polynomial System Solving Paris, November 24-25-26 2004 in honor of Daniel Lazard", 2004.

[46] T. P. BERGER, P. LOIDREAU. *Designing an Efficient and Secure Public-Key Cryptosystem Based on Reducible Rank Codes*, in "Proceedings of INDOCRYPT 2004", Lecture Notes in Computer Science, 2004.

[47] T. BERGER, A. OURISKI. *Construction of new MDS codes from Gabidulin codes*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 40-47.

[48] V. BÉNONY, F. RECHER, E. WEGRZYNOWSKI, C. FONTAINE. *An improved method to retrieve internal state of Klimov-Shamir pseudo-random sequence generators*, in "Sequences and their applications – SETA 2004", to appear, 2004.

[49] C. CARLET. *On the secondary constructions of resilient and bent functions*, in "Coding, Cryptography and Combinatorics", Progress in Computer Science and Applied Logic, vol. 23, Birkhäuser Verlag, Basel, 2004, p. 3-28.

[50] C. CARLET, P. CHARPIN. *Cubic Boolean functions with highest resiliency*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 497.

[51] C. CARLET, P. GABORIT. *Hyper-bent functions and cyclic codes*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 499.

[52] C. CARLET, E. PROUFF. *Vectorial Functions and Covering Sequences*, in "Finite Fields and Applications, Fq7", A. P. G. L. MULLEN, H. S. EDTS (editors)., Lecture Notes in Computer Science, vol. 2948, 2004, p. 215-248.

[53] F. CAYRE, C. FONTAINE, T. FURON. *Watermarking Attack: Security of WSS Techniques*, in "International Workshop on Digital Watermarking – IWDW 2004", Lecture Notes in Computer Science, à paraître, Best Paper Award, Springer-Verlag, 2004.

[54] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *On binary BCH codes with minimal distance 8 and Kloosterman sums*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 90-94.

[55] M. CLUZEAU. *Reconstruction of a linear scrambler*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 230.

[56] L. DUBREUIL, T. BERGER. *Spread spectrum, cryptography and information hiding*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 143-48.

[57] E. FILIOL. *Evolution des idées en virologie informatique*, in "7ème Colloque d'Histoire de l'Informatique et de télécommunications, Rennes, CHIR 2004", to appear, 2004.

[58] E. FILIOL, C. F. S. JOSSE. *The COSvd Ciphers*, in "The State of the Art of Stream Ciphers, ECRYPT, Brugges, Belgium", October 2004.

[59] E. GABIDULIN, P. LOIDREAU. *On subspaces subcodes of rank codes*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 178-84.

[60] P. GABORIT, C. S. NEDELOAIA, A. WASSERMANN. *Weight enumerators of duadic and quadratic residue codes*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", june 2004, 485.

[61] G. KABATIANSKY, C. TAVERNIER. *List decoding of Reed-Muller codes*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 230-35.

[62] F. LEVY-DIT-VEHEL, L. PERRET. *A Polly Cracker System Based on Satisfiability*, Progress in Computer Science and Applied Logic, vol. 23, Birkhäuser Verlag, Basel, 2004, p. 177-192.

[63] F. LEVY-DIT-VEHEL, L. PERRET. *Attacks on Public-Key Cryptosystems Based on Free Partially Commutative Monoids and Groups*, in "Advances in Cryptology - INDOCRYPT 2004", Lecture Notes in Computer Science, to appear, Springer-Verlag, 2004.

[64] P. LOIDREAU, B. SAKKOUR. *Modified version of Sidelnikov-Peshakov decoding algorithm for binary second order Reed-Muller codes*, in "Proceedings of ACCT'9, Kranevo, Bulgaria", June 2004, p. 266-72.

[65] W. MEIER, E. PASALIC, C. CARLET. *Algebraic attacks and decomposition of Boolean functions*, in "Advances in Cryptology - EUROCRYPT 2004", Lecture Notes in Computer Science, n° 3027, Springer-Verlag, 2004, p. 474-491.

[66] M. MINIER. *A three rounds property in the AES*, in "Proceedings of the fourth conference on the AES", to appear, Lecture Notes in Computer Science, Springer-Verlag, 2004.

[67] L. PERRET, A. BAYAD. *A differential approach to a polynomial equivalence problem*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 142.

[68] L. PERRET. *A Geometrical Approach to a Polynomial Equivalence Problem*, in "Procceedings of the International Conference on Polynomial System Solving (ICPSS), Paris", nov 2004.

[69] N. SENDRIER. *Linear codes with complementary duals meet the Gibert-Varshamov bound*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 456.

[70] J. TILLICH. *The average weight distribution of Tanner code ensembles and a way to modify then to improve*

their weight distribution, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 7.

[71] M. VIDEAU. *On some properties of symmetric Boolean functions*, in "Proceedings 2004 IEEE International Symposium on Information Theory, Chicago,USA", June 2004, 500.

Internal Reports

[72] E. FILIOL. *Strong Cryptography Armoured Computer Viruses Forbidding Code Analysis: the bradley virus*, Rapport de recherche, n° RR-5250, INRIA, June 2004, http://www.inria.fr/rrrt/rr-5250.html.

[73] Y. LAIGLE-CHAPUY. *Les polynômes de permutation. Applications en théorie des codes*, rapport de stage, DEA "Algorithmique", Technical report, INRIA, Juin 2004.

[74] F. LEVY-DIT-VEHEL, L. PERRET. *Polynomial Equivalence Problems and Applications to Multivariate Cryptosystems*, Rapport de recherche, n° RR-5119, INRIA, Février 2004, http://www.inria.fr/rrrt/rr-5119.html.

[75] M. MINIER. *A bottleneck attack on Crypton*, Rapport de recherche, n° RR-5324, INRIA, October 2004, http://www.inria.fr/rrrt/rr-5324.html.

[76] R. TRIKI. *Application de techniques de décodage à la cryptanalyse de systèmes de chiffrements*, rapport de stage, DEA "Algorithmique", Technical report, INRIA, Juin 2004.

Miscellaneous

[77] R. BHASKAR. *Group Key Agreement in Ad hoc Networks*, Journées "Codage et Cryptographie", Aussois, France, Février 2005.

[78] S. MANUEL. *Codes d'authentification de messages - Application aux fonctions de hachage fondées sur le décodage de syndrome rapide*, Rapport de stage de maîtrise, Université Paris 8, October 2004.