INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Codes

Codage et cryptographie

Rocquencourt

THEME 2B

Table of contents

1. Team **1**
2. Overall Objectives **1**
2.1. Présentation 1
3. Scientific Foundations **2**
3.1. Fondements 2
6. New Results **3**
6.1. Étude et analyse de structures discrètes 3
6.1.1. Groupes d'automorphismes 3
6.1.2. Codes cycliques et codes auto-duaux 3
6.1.3. Duaux des codes BCH 4
6.1.4. Codes de Goppa 4
6.1.5. Codes sur des anneaux 4
6.1.6. Recherche de mots de poids faible dans un code 4
6.1.7. Construction de nouveaux codes à partir des codes de Gabidulin. 4
6.1.8. Séquences et CDMA 5
6.2. Cryptographie à clé publique 5
6.2.1. Système de chiffrement utilisant des codes correcteurs 5
6.2.2. Fonction de hachage basée sur le problème du décodage 5
6.2.3. Implantation de cryptosystèmes basés sur les codes correcteurs 5
6.2.4. Cryptosystèmes basés sur des problèmes combinatoires 6
6.2.5. Cryptosystèmes basés sur des problèmes algébriques 6
6.2.6. Signature par le "Extended Domain Hash" 6
6.2.7. Sécurisation d'applications partagées 7
6.3. Algorithmes de décodage 7
6.4. Reconnaissance de codes 8
6.5. Primitives du chiffrement symétrique 8
6.5.1. Fonctions booléennes 8
6.6. Étude et conception de cryptosystèmes pour les réseaux de télécommunication 9
6.7. Chiffrement symétrique : cryptanalyse 10
6.7.1. Cryptanalyse des chiffrements par blocs 10
6.7.2. Décodage et cryptanalyse 10
6.7.2.1. Chiffrement par bloc 10
6.7.3. Cryptanalyse des chiffrements à flot 11
6.7.4. Attaques considérant la forme algébrique normale 11
6.7.5. Testeurs 12
6.7.6. Cryptanalyse et tatouage 12
6.8. Génération logicielle de nombres aléatoires 12
6.8.1. Par l'entropie intrinsèque aux calculateurs 12
6.8.2. Par les nombres 2-adiques 13
6.8.2.1. Automates non linéaires 13
6.9. Protection des droits d'auteurs – watermarking 13
6.10. Informatique quantique 13
7. Contracts and Grants with Industry **14**
7.1.1. Contrat avec Canal+Technologies 14
7.1.2. Collaboration France-Télécom RD-INRIA-LACO : 14
7.1.3. Contrat DGA-CELAR 14
7.1.4. Contrat DGA 14

8. Other Grants and Activities **14**
8.1. Actions nationales 14
8.1.1. Contrats nationaux 14
8.1.1.1. CrAC – Action Concertée Incitative “Cryptologie” (2000-2003) 14
8.1.1.2. Crac II 15
8.1.1.3. ACI PolyCrypt 15
8.1.1.4. ACI ACCESS (Outils algébriques et combinatoires pour la construction et l’étude de systèmes à clé publique) 15
8.1.1.5. RNRTs 15
8.1.1.6. sixième PCRD européen 15
8.1.2. Groupes de recherche 15
8.1.3. Participations à des instances et manifestations nationales 16
8.2. Actions internationales 16
8.2.1. Organisation de rencontres 16
8.2.2. Accueils de chercheurs étrangers 17
9. Dissemination **17**
9.1. Enseignement 17
9.2. Jurys de thèse 18
9.3. Participation à des colloques 18
10. Bibliography **19**

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]
Caroline Fontaine [Université Lille]
Philippe Gaborit [Université Limoges]
Françoise Levy-dit-Vehel [ENSTA]
Pierre Loidreau [ENSTA]

Post-doctorants
Emmanuel Cadic

Doctorants
Magali Bardet-Turel [AMN]
Raghav Bhaskar [Bourse Égide]
Mathieu Cluzeau [Bourse DGA]
Matthieu Finiasz [AMN]
Fabien Galand [Bourse BDI]
Cédric Lauradoux [Bourse INRIA]
Carmen Nedeloaia [Bourse régionale]
Harold Ollivier [X-Telecom]
Ludovic Perret [Bourse MESR]
Gregory Olocco [Bourse MESR]
Emmanuel Prouff [ATER Orsay]
Cédric Tavernier [Bourse DGA]
Marion Videau [Bourse DGA]

Stagiaires
Thomas Camara [Stage de DEA, Université de Paris 6, de mars à août 2003]
Mathieu Cluzeau [Stage de DEA, Université de Limoges, de mars à juillet 2003]
Vivien Dubois [Stage d'option de fin d'études, LIX, d'avril à juillet 2003]
Thomas Roetynck [Stage d'option, ENST Bretagne, de juillet à septembre 2003]

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 qúils 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 qúapplication 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 qúappliqués 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

[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.

domaine des télécommunications apparaissent qui justifient le développement d'une communauté possédant une palette large de compétences. Ceci apparaît dans les activités d'un nombre croissant de laboratoires de recherche dans le monde. Une étude récente de la NSF américaine [2] montre aussi la reconnaissance d'un nouveau domaine de recherche ainsi qu'une volonté institutionnelle de coordonner les efforts.

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

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

6. New Results

6.1. Étude et analyse de structures discrètes

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

6.1.1. Groupes d'automorphismes

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 basés sur le métrique "rang", différente de la métrique de Hamming usuellement considérée. Pour cette métrique il a défini la notion d'isomorphisme et étudié les isométries de codes de Gabidulin et des codes hyperboliques. Il a caractérisé les groupes d'isométries et les groupes de permutations des codes de Gabidulin.

6.1.2. Codes cycliques et codes auto-duaux

Participants: Carmen Nedeloaia, Pascale Charpin, Philippe Gaborit.

Les travaux précédents de Carmen Nedeloaia sur les codes auto-duaux se sont achevés, avec la publication [25].

Philippe Gaborit a étudié comment construire des codes auto-duaux à partir de la méthode de construction de la famille des codes dits CORTEX. Cela a permis entre autres de construire un nouveau code de paramètres non-connus avant : un code [114,57,16] sur GF(2) [21] (un code [92,46,16] sur GF(2), un code [52,26,15] sur GF(3) ou encore un code [46,23,14] sur GF(4) ayant déjà été trouvés en 2002.

Il a étudié de nouveaux designs contenus dans certains codes auto-duaux, et en particulier a montré dans [5], l'existence de 1-designs ou 2-designs inconnus auparavant dans certains codes s-extrêmaux ayant la particularité d'avoir une ombre longue. Philippe Gaborit a construit un algorithme de décodage élémentaire et "à la main" du code RM(2,5) simplement à partir d'une description combinatoire de ses éléments [20].

Du point de vue combinatoire il a construit de nouveaux réseaux unimodulaires en dimensions supérieures à la dimension à partir de codes auto-duaux et de la construction "A" ou à partir d'une construction par

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

voisinage [19], en particulier il a obtenu le premier réseau unimodulaire de norme 6 en dimension, avec la série theta correspondante.

Philippe Gaborit et Carmen Nedeloaia ont aussi réussi à calculer le polynôme énumérateur des poids des codes de résidus quadratiques jusqu'à la longueur 152.

6.1.3. 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.

6.1.4. 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 basés sur les codes correcteurs d'erreurs.

6.1.5. Codes sur des anneaux

Participants: Gabien 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.

6.1.6. 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.

6.1.7. Construction de nouveaux codes à partir des codes de Gabidulin.

Participant: Thierry Berger.

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.

6.1.8. 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).

6.2. Cryptographie à clé publique

6.2.1. Système de chiffrement utilisant des codes correcteurs

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

Dans ce thème sont regroupées l'étude et la conception de systèmes de chiffrement où interviennent des codes correcteurs. Les clés utilisées sont en général publiques. Ces systèmes sont fondés sur des problèmes *durs* de théorie des codes, essentiellement décoder et/ou identifier un code dont la structure ou les paramètres sont cachés.

Matthieu Finiasz et Daniel Augot ont inventé un nouveau système de chiffrement à clé publique, basé sur la difficulté de reconstruire un polynôme d'après ses valeurs "bruitées". Ce système présente des clés plus courtes que le système de McEliece, mais les blocs de chiffrements sont beaucoup plus longs. Ce système a été présenté à la conférence Eurocrypt à Varsovie [32]. Il a été cassé par Jean-Sébastien Coron ; une réparation a été proposée en collaboration avec Pierre Loidreau [50]. Cette réparation a de nouveau été cassée par Jean-Sébastien Coron.

6.2.2. Fonction de hachage basée 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.

6.2.3. Implantation de cryptosystèmes basés 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 à 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.

6.2.4. Cryptosystèmes basés sur des problèmes combinatoires

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

L'activité de Françoise Levy-dit-Vehel, Pierre Loidreau et de Ludovic Perret à l' ENSTA se concentre autour de l'ACI ACCES, à travers deux axes. Françoise Levy-dit-Vehel et Ludovic Perret étudient des méthodes de construction de cryptosystèmes à clef publique basés sur des problèmes difficiles de combinatoires. Dans ce cadre, le premier problème étudié a été celui de la satisfaisabilité des ensemble de clauses à trois littéraux (3-SAT). Ainsi, le travail autour des schémas de type Polly Cracker a donné lieu à la publication d'un article à la conférence CCC [44]. Nous envisageons de poursuivre l'étude de ces schémas en nous concentrant davantage sur le problème sous-jacent du test d'appartenance à un idéal.

Comme toujours en cryptographie, l'autre versant de la recherche est l'étude d'algorithmes pour casser les systèmes proposés. Le deuxième axe développé plus récemment est l'étude et la mise en oeuvre d'algorithmes de résolution du problème connu sous le nom d'"isomorphisme de polynômes", mais que nous préférons appeler "équivalence polynômiale". Nous avons proposé dans [45] deux algorithmes de résolution de ce problème, basés sur des calculs de variétés associées aux idéaux engendrés par les polynômes considérés. Ces algorithmes s'avèrent très efficaces pour des choix de paramètres utilisés dans des schémas cryptographiques, et en constituent donc des méthodes de cryptanalyse. D'autres méthodes de résolution sont en cours d'investigation.

6.2.5. Cryptosystèmes basés sur des problèmes algébriques

Participants: Daniel Augot, Magali Bardet, Philippe Gaborit.

Daniel Augot encadre Magali Bardet qui est codirigée par Jean-Charles Faugère du LIP6, spécialiste de la résolution de systèmes d'équations algébriques. L'axe de recherche ici étudié est la 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 polynômiaux 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). 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).

6.2.6. 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.

6.2.7. 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, qui est en cours d'analyse, du point de vue de la sécurité.

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

6.3. Algorithmes de décodage

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

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

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. Nous avons 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, nous proposons 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 nous pouvons également appliquer cette amélioration à la famille des codes LDPC, et là aussi nous améliorons les performances du décodage itératif à fort rapport signal à bruit.

Grégory Olocco et Jean-Pierre Tillich s'intéressent aux apports des techniques de décodage itératif dans le domaine des codes correcteurs d'erreur. L'intérêt de ce type de décodage est qu'il approxime remarquablement le décodage optimal au maximum de vraisemblance pour une très large classe de codes, et reste de complexité algorithmique tout à fait raisonnable. Nous avons commencé par étudier, dans le cadre d'un contrat entre le CCETT et l'INRIA, le décodage itératif d'une nouvelle famille de codes brevetés par le CCETT, les codes cortex, et nous avons montré par une analyse théorique, comment choisir les paramètres de ces codes afin d'optimiser les performances du décodage itératif. Grégory Olocco a soutenu sa thèse en 2003.

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

Décodage "dur" de codes de Reed et Muller : dans le but d'applications cryptographiques, Cédric Tavernier essaye d'améliorer un algorithme du a Goldreich, Rubinfeld et Sudan qui permet de décoder ces codes. Cet algorithme ne fonctionne pas quand le corps est trop petit, notamment dans le cas binaire qui est le plus

important en pratique. Cédric Tavernier essaye de mélanger cette approche avec celle de Dumer, qui construit un décodage récursif des codes de Reed-Muller. L'objectif est de pouvoir décoder au delà de la distance minimale. 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.

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

6.4. 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.

6.5. Primitives du chiffrement symétrique

6.5.1. Fonctions booléennes

Participants: Claude Carlet, Pascale Charpin, Anne Canteaut.

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*.

C. Carlet, avec Emmanuel Prouff, a caractérisé les fonctions courbes et les fonctions dites 3-valuées à l'aide des séquences couvrantes. Ils ont généralisé la notion de séquence couvrante aux fonctions booléennes à sortie multiple (fonctions vectorielles), après avoir fait le point de l'état de l'art et amélioré certains résultats en matière de constructions de telles fonctions (article à paraître dans les actes du congrès Fq7). Ils ont aussi étudié une nouvelle notion de non-linéarité pour les fonctions vectorielles utilisées dans les générateurs de pseudo-aléas.

La construction générale de fonctions courbes et résilientes connue sous le nom de Maiorana McFarland était encore récemment la seule connue qui permette de construire en nombres importants des fonctions courbes ou des fonctions résilientes présentant d'autres qualités cryptographiques telles qu'une bonne non-linéarité. C. Carlet a obtenu une borne supérieure efficace sur la non-linéarité de ces fonctions et il a mis en évidence divers paramètres qu'elles permettent d'obtenir. Il a également montré qu'il est possible d'obtenir

des résultats similaires et parfois meilleurs en concaténant des fonctions quadratiques. Avec Emmanuel Prouff, il a introduit une autre construction de concaténations de fonctions quadratiques, dont les paramètres cryptographiques peuvent être également calculés.

Avec Cunsheng Ding (Université de Hong-Kong), C. Carlet a rédigé un article résumant et généralisant l'état de l'art en matière de non linéarité parfaite des fonctions définies et à valeurs dans des groupes abéliens (un article de 44 pages accepté pour publication dans la Special Issue du Journal of Complexity dédiée aux 60 ans de H. Niederreiter).

Les fonctions booléennes cryptographiques doivent avoir un niveau de complexité aussi élevé que possible pour satisfaire au principe de confusion de Shannon. C. Carlet en a formalisé deux nouveaux critères de conception de fonctions booléennes. L'un, qu'il a appelé l'épaisseur algébrique, est lié au nombre de termes dans la forme algébrique normale des fonctions linéairement équivalentes à la fonction considérée. L'autre est lié à la dimension minimale des sous-espaces affines sur lesquels la fonction est constante ou affine. Il a mené l'étude de ces deux critères, en liaison avec la non linéarité et le degré. Il a montré que, comme en complexité de circuit, presque toutes les fonctions booléennes sont simultanément de haute complexité relativement aux 4 critères. Il a ensuite amélioré ces résultats dans un article présenté au congrès "2003 IEEE Information Theory Workshop".

C. Carlet a étudié avec A. Klapper une construction de familles de séquences offrant un bas niveau de corrélations croisées. Ces familles sont utiles en télécommunication CDMA (un article publié par IEEE Transactions on Information Theory).

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

– *Les propriétés descendantes des fonctions courbes*[3]. L'idée générale de ce travail est d'introduire un élément de classification des fonctions courbes par le biais de leurs décompositions. Ce point de vue semble pertinent compte tenu de nos premiers résultats sur les décompositions par rapport aux espaces de codimension 2 : une grande diversité apparaît qui n'est pas dans le cadre des classes établies.

– *La normalité des Fonctions Booléennes.* 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. Des résultats récents sur les décomposition des fonctions permettent aussi d'optimiser les algorithmes de recherche de normalité.

Les propriétés de normalité (et de normalité faible) dans le cas particulier des fonctions courbes ont été étudiées par A. Canteaut, M. Daum, H. Dobbertin et G. Leander. Ils ont notamment montré que la plupart des grandes familles connues de fonctions courbes, ainsi que celles obtenues par des constructions secondaires, sont normales. Un résultat important de ce travail est la mise en évidence pour la première fois d'une fonction courbe non normale et non faiblement normale, ce qui répond à un problème ouvert formulé en 1995.

Philippe Gaborit a récemment proposé à Eurocrypt une famille de fonctions contenues dans l'ensemble des fonctions courbes et possédant des propriétés encore plus spécifiques: les fonctions hyper-bents. Il s'intéresse à ces fonctions et montre entre autres que dans beaucoup de cas ces fonctions se limitent aux fonctions "partial spread" de Dillon et qu'elles sont nécessairement de degré fixé.

6.6. 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

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

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.

6.7. Chiffrement symétrique : cryptanalyse

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

6.7.1. 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.

6.7.2. Décodage et cryptanalyse

6.7.2.1. 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. C. 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.

6.7.3. 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.

6.7.4. Attaques considérant la forme algébrique normale

L'attaque des systèmes de chiffrement symétriques, essentiellement basée sur une approche combinatoire qui permet de trouver une information de nature plus qualitative que quantitative. L'angle 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 traduite de sorte à retrouver "facilement" des bits d'information sur la clef. Les résultats obtenus sont très prometteurs et ont fait l'objet d'une soumission à FSE 2003.

6.7.5. 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 $f : F_q \rightarrow F_q$. Le testeur est un algorithme probabiliste, utilisant f comme oracle et devant répondre à la question “f est-elle proche d'un polynôme de base degré.

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

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

6.7.6. Cryptanalyse et tatouage

Les travaux de Caroline Fontaine sur les liens entre tatouage et cryptographie ont mis à jour plusieurs sujets de recherche. Le plus original et le plus intéressant est l'étude d'attaques structurelles sur les algorithmes de tatouage, visant non pas à lessiver le filigrane, mais à retrouver la clé secrète utilisée lors de son insertion (personne d'autre n'a abordé cette question). Caroline Fontaine collabore sur ce thème avec Teddy Furon, à l'IRISA. Ils travaillent principalement à l'attaque des schémas reposant sur l'étalement de spectre. Le travail a commencé par une étude pratique pour aboutir à des attaques efficaces et réelles ; ils vont en parallèle mener une étude théorique, *à la Shannon*. Ces recherches ont débuté à l'automne 2002, et ont conduits à l'analyse d'articles traitant de séparation de sources. Ils sont en train établir les liens précis entre le problème de départ, et cette branche du traitement du signal.

6.8. Génération logicielle de nombres aléatoires

6.8.1. 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 [30]. 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.

6.8.2. 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.

6.8.2.1. 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.

6.9. Protection des droits d'auteurs – watermarking

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

Suite aux travaux sur le projet européen AQUARELLE, le thème du marquage d'images est resté dans le projet. Les participants sont C. Fontaine (LIFL) et Fabien Galand.

Caroline Fontaine est partenaire d'un projet RNRT, appelé SDMO (Secure Diffusion of Music on mObiles); ce projet vise à étudier la possibilité de sécurisation de la diffusion de morceaux de musique sur les téléphones mobiles 3G. Il a commencé en janvier 2003, et n'en est donc qu'à ses débuts. Caroline Fontaine est en charge du sous-projet *sécurité*, dont le rôle est de définir l'architecture de sécurité, ainsi que de fournir une analyse complète de la sécurité finale du projet, tant au niveau cryptographique qu'en ce qui concerne le tatouage. Un post-doc devrait être recruté dans l'année pour travailler sur ce projet, d'une durée totale de trente mois.

En parallèle, Fabien Galand 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 basé 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[4] 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).

6.10. Informatique quantique

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

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

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

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.

7. Contracts and Grants with Industry

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

7.1.1. Contrat avec Canal+Technologies

Expertise d'un algorithme de chiffrement. (Sept. 2002 – Mars 2003). Anne Canteaut et Daniel Augot.

7.1.2. Collaboration France-Télécom RD-INRIA-LACO :

Étude de nouveaux turbo-codes en bloc les codes CORTEX, 99-2001, demandé à être prolongé en 2002, puis en 2003.

Les responsables sont : T. Berger (LACO), J.P. Tillich (INRIA) et J.-C. Carlach (France-Télécom-RD).

Un post-doc Emmanuel Cadic a été recruté pour 2003-2004.

7.1.3. Contrat DGA-CELAR

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

7.1.4. 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.

8. Other Grants and Activities

8.1. 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.

8.1.1. Contrats nationaux

8.1.1.1. 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".

8.1.1.2. 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 75 000 Euros sur une durée de trois ans à partir d'août 2002.

8.1.1.3. 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.

8.1.1.4. ACI ACCESS (Outils algébriques et combinatoires pour la construction et l'étude de systèmes à clé publique)

Cette ACI obtenue par Françoise Levy-dit-Vehel et Pierre Loidreau est gérée par le projet Codes, qui y est ainsi impliqué.

8.1.1.5. 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 SDMO (Secure Diffusion of Music on mObiles). Responsable : Caroline Fontaine.
- RNRT DIPHONET (DIffusion de PHOtographies à travers (I)nterNET - projet précompétitif. Responsable : Françoise Levy-dit-Véhel.

8.1.1.6. 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".

8.1.2. Groupes de recherche

Le projet participe à :

- GDR *Algorithmes Langages et Programmation* (AMI) : Claude Carlet a la responsabilité du groupe de travail intitulé *Codage et Cryptographie*.
- au GDR Information quantique (Harold Ollivier).
- GDR ISIS : Information, Signal, Images et ViSion (Caroline Fontaine)

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[5] depuis octobre 99.

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

8.1.3. Participations à des instances et manifestations nationales

Plusieurs membres du projet participent à des commissions de spécialistes :

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

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 membre de la commission de spécialiste 25-26-27-72-ièmes section de Paris VIII, 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.

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

8.2. Actions internationales

8.2.1. Organisation de rencontres

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

Organisation de rencontres internationales :

- A. Canteaut est membre des comités de programme de FSE 2003, du 2003 IEEE Information Theory Workshop (ITW), de Indocrypt 2003, de Crypto 2004, YACC 2004, Indocrypt 2004.
- N. Sendrier est membres du comité de programme du IEEE Information Theory Workshop, Paris, 31 mars - 4 avril 2003.
- Presque tous les membres du projet ont organisé le colloque international WCC'03 *Workshop on Coding and Cryptography 2003*, 24-28 mars 2003, Versailles, France. Le comité de programme est présidé par P. Charpin (co-présidence avec G. Kabatianski) et le comité d'organisation par P. Loidreau. Il y a eu 107 soumissions, (cf. http://www-rocq.inria.fr/codes/WCC2003), et environ 150 participants. Ce colloque, organisé tous les deux ans, est un grand succès.
- P. Gaborit est organisateur des journées annuelles de Cryptographie et de Sécurité de l'information de Limoges (120 participants).
- C. Carlet est membre du comité de programme de WCC2003 (Workshop on Coding and Cryptography), de AAECC (Applied Algebra, Algebraic Algorithms, and Error Correcting Codes), et de Fq7 (Finite Fields and Applications)
- T. Berger est membre du comité scientifique de AAECC, et de la troisième école d'été « CSA 03 » , Cryptologie, Sécurité, Applications, Rabat, septembre 2003.
- N. Sendrier a organisé la session cryptographie aux « Journées Nationales de Calcul Formel 2003 », Luminy, janvier 2003.

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.

8.2.2. Accueils de chercheurs étrangers

- An Braeken, Université de Leuven, Belgique ;
- Reiner Steinwandt, IAKS, Université de Karlsruhe, Allemagne ;
- Igor Spharlinski, Université de Macquarie, Australie.
- Ernst Gabidulin, Institute of Physics and Technology, Dept. of Radio, Moscou, Russie ;
- Gregory Kabatiansky, IPIT, Moscou, Russie ;
- Gintaras Skersys, Université de Vilnius, Lituanie ;
- Victor Zinoviev, IPIT, Moscou, Russie ;

9. Dissemination

9.1. Enseignement

Pour les écoles doctorales, notre activité est d'abord une collaboration concrète avec nos chercheurs extérieurs sur le contenu des cours, les sujets de recherche et l'encadrement des thésards et stagiaires. Outre les DEA de Caen, Limoges et Toulon, nous sommes particulièrement impliqués dans le DEA parisien : *Algorithmique*, X-Ulm et universités Paris-centre. Filière *Traitement et Protection de l'Information*. Précisément, les enseignements ou cours de formation permanente cette année ont été:

- T. Berger est responsable de la formation doctorale de mathématiques de l'Université de Limoges.
- T. Berger est membre du bureau de l'école doctorale Science, Technologie, Santé de Limoges.
- Daniel Augot et Jean-Pierre Tillich interviennent dans le DEA Algorithmique, filière Traitement et protection de l'Information, pour assurer un cours de codes correcteurs d'erreurs.
- J.P. Tillich intervient dans le DESS d'ingénierie Mathématique de l'Université de Paris-Sud.
- J.P. Tillich est responsable du cours "Algorithmique, programmation et complexité" en licence d'informatique à l'Université de Paris-Sud.
- A. Canteaut enseigne la *programmation en langage* C dans le DEA *Cryptographie, Codage, Calcul* et dans le DESS *Sécurité de l'information* de l'Université de Limoges. Ce cours met en particulier l'accent sur les techniques algorithmiques spécifiques à la cryptographie et au codage.
- N. Sendrier est chargé d'enseignement à l'École Polytechnique au département d'informatique. Cours enseignés : Algorithmique et programmation (travaux dirigés), Introduction à la théorie de l'information (cours + TD).
- TPs de cryptographie, P. Loidreau à l'ENSTA.
- F. Levy-dit-Vehel enseigne un cours "Primitives cryptographiques" en troisième année à l'ENSTA, elle a aussi donné un exposé "Introduction à la cryptographie' à l'École thématique du CNRS VCARS.

9.2. Jurys de thèse

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

Mars 2003 J. Ryan, Thèse d'Université de Cork, Ireland *Irreducible Goppa Codes*. Jury : T. Berger (external examinator).

Avril 2003 G. Olocco, *Décodage itératif et distance minimale d'une nouvelle famille de codes auto-duaux*. Thèse d'Université de Jury : T. Berger (rapporteur), P. Charpin (directeur), J.P. Tillich (co-directeur).

Mai 2003 E. Thomé, Thèse d'Université, École Polytechnique, *Algorithmes de calcul du logarithme discret dans les corps finis* Jury : T. Berger (rapporteur).

Mai 2003 J.Y. Enjalbert, Thèse d'Université de Limoges, *Jacobiennes et cryptographie*. Jury : T. Berger (co-directeur).

Octobre 2003 E. Cadic, Thèse d'Université de Limoges, *Construction de turbocodes possédant de bonnes propriétés de distance minimale*. Jury : T. Berger (co-directeur), P. Charpin (rapporteur), J.P. Tillich.

9.3. Participation à des colloques

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

Séjours courts dans des universités ou laboratoires en 2003 :

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

Participations aux colloques en 2003 :

- Journées Nationales de Calcul Formel, Luminy, Marseille, France, 20 au 24 janvier 2003. D. Augot, N. Sendrier.
- École de Cryptologie, Bordeaux, France, 3 au 7 février 2003. F. Galand, M. Videau.
- FSE (Fast Software Encryption), Lund, Suède, 24 au 26 février 2003. A. Canteaut, C. Carlet, P. Charpin, M. Videau.
- Nessie/Stork Workshop, Lund, Suède, 26 au 27 février 2003. A. Canteaut, C. Carlet, M. Videau.
- IEEE Information Theory Workshop, Paris, 30 mars au 4 avril 2003. C. Carlet, F. Galand, J.-P. Tillich.
- FQ7 (Finite Fields), Toulouse, France, 5 au 9 mai 2003. C. Carlet.
- WCC'03, Rocquencourt, France, 24 au 28 mars 2003.
  Comité de programme : D. Augot, C. Carlet, P. Charpin.
  Comité d'organisation : A. Canteaut, E. Filiol, C. Fontaine, P. Gaborit, F. Lévy-dit-Véhel, P. Loidreau, N. Sendrier, J.-P. Tillich.
  Participants : R. Bhaskar, M. Finiasz, F. Galand, G. Olocco, H. Ollivier, E. Prouff, G. Skersys, C. Tavernier, M. Videau.
- EUROCRYPT'03, Varsovie, Pologne, 4 au 8 mai 2003. D. Augot, M. Finiasz, F. Levy-dit-Véhel.

- AAECC15 (Applicable Algebra Error Correcting Codes), Toulouse, France, 11 au 15 mai 2003. F. Galand.
- ISIT'03 (IEEE International Symposium on Information Theory), Yokohama, Japon, 29 juin au 4 juillet 2003. M. Bardet, M. Finiasz, F. Galand, P. Loidreau.
- Resa Meeting, Garshing, Allemagne, 11 au 15 mai 2003. H. Ollivier.
- Quantum Information and Communication Workshop, Benasque, Espagne, 22 juin au 12 juillet 2003. H. Ollivier.
- CRYPTO'03, 17 au 21 août 2003, Santa Barbara, USA. M. Finiasz, N. Sendrier.
- 3rd International Symposium on Turbo Codes and Related Topics, Brest, France, 1er au 5 septembre 2003. J-P. Tillich.
- Conférence interne INRIA Réseaux Dynamiques, Porquerolles, France. 8 au 10 septembre 2003. D. Augot, R. Bhaskar.
- Workshop Air and D - Réseaux ad Hoc et Sécurité, 7 au 8 octobre 2003, Saint-Malo, France. D. Augot.
- INDOCRYPT'03, New Delhi, Inde, 8 au 10 décembre 2003. Comité de programme : A. Canteaut. F. Levy-dit-Véhel, L. Perret.
- Conference on Mathematics of Communication, Moscou, Russie, 3 au 7 novembre 2003. P. Loidreau.
- Conference PASI'03, Rio de Janeiro, Brésil, 30 novembre au 14 décembre 2003. H. Ollivier.
- 4ème Journée Cryptographie et Sécurité de l'Information, Limoges, France, 27 au 30 novembre 2003. M. Cluzeau.
- Ninth IMA Conference Cryptography and Coding, Cirencester, UK, 16 au 18 décembre 2003. Conférencier : Enes Pasalic.

10. Bibliography

Books and Monographs

[1] C. CARLET, editor, *Revue Discrete Applied Mathematics - Special issue in Coding and Cryptology.* volume 128, Issue 1, Elsevier, May, 2003, Éditeurs associés : M. Girault (France Telecom R&D-Caen), T. Helleseth (Bergen, Norvège), T. Hohøldt (Lyngby, Danemark), F. Morain (École Polytechnique, Palaiseau), N. Sendrier (INRIA-Rocquencourt).

[2] É. FILIOL, editor, *Les virus informatiques : théorie, pratique et applications.*. volume XXIV, 388, ISBN 2-287-20297-8, Collection Iris, Springer Verlag, Novembre, 2003.

Doctoral dissertations and "Habilitation" theses

[3] G. OLOCCO. *Décodage itératif et distance minimale d'une nouvelle famille de codes auto-duaux.* Thèse de doctorat, Université Paris-Sud, Orsay, Avril, 2003.

Articles in referred journals and book chapters

[4] D. AUGOT. *Les travaux de Madhu Sudan sur les codes correcteurs d'erreurs.* in « La gazette des mathématiciens », Octobre, 2003.

[5] C. BACHOC, P. GABORIT. *Designs and self-dual codes with long shadows.* in « Jour. Comb. Theory Series A », 2003, to appear.

[6] T. BERGER. *Isometries for rank distance and permutation group of Gabidulin codes.* in « IEEE Trans. Inform. Theory », number 11, volume 48, 2003, pages 3016-3019.

[7] T. P. BERGER, P. LOIDREAU. *How to mask the structure of codes for a cryptographic use.* in « Designs, Codes and Cryptography », 2003, to appear.

[8] N. BRULEZ, É. FILIOL. *Analyse d'un ver ultra-rapide : Sapphire/Slammer.* in « MISC - Le journal de la sécurité informatique », volume 8, Juillet, 2003.

[9] A. CANTEAUT, P. CHARPIN. *Decomposing Bent Function.* in « IEEE Trans. Inform. Theory », number 8, volume 49, August, 2003, pages 2004-19.

[10] 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 », 2003, Special Issues on Complexity Issues in Cryptography and Coding Theory..

[11] C. CARLET, C. DING. *Highly Nonlinear Mappings.* in « Journal of Complexity », 2003, Special Issues on Complexity Issues in Cryptography and Coding Theory".

[12] P. CHAMBET, É. FILIOL, E. DETOISIEN. *La fuite d'informations dans les documents propriétaires.* in « MISC - Le journal de la sécurité informatique », volume 7, Mai, 2003.

[13] P. CHARPIN. *Normal Boolean functions.* in « Journal of Complexity », volume Special Issues on Complexity Issues in Cryptography and Coding Theory, 2003, to appear..

[14] É. FILIOL. *La lutte antivirale : techniques et enjeux.* in « MISC - Le journal de la sécurité informatique », volume 5, January, 2003.

[15] É. FILIOL. *Les infections informatiques.* in « MISC - Le journal de la sécurité informatique », volume 5, January, 2003.

[16] É. FILIOL. *Les virus informatiques.* in « Techniques de l'ingénieur - Sécurité informatique », Novembre, 2003, to appear.

[17] É. FILIOL. *Un virus de boot furtif : STEALTH.* in « MISC - Le journal de la sécurité informatique », volume 6, Mars, 2003.

[18] É. FILIOL, F. RAYNAL. *La sécurité du WEP.* in « MISC - Le journal de la sécurité informatique », volume 6, Mars, 2003.

[19] P. GABORIT. *Construction of new unimodular lattices.* in « European Journal of Combinatorics », 2003, to appear.

[20] P. GABORIT, J.-L. KIM, V. PLESS. *Decoding binary $R(2,5)$ by hand.* in « Discrete Mathematics », number 1–3, volume 264, 2003, pages 55–73.

[21] P. GABORIT, A. OTMANI. *Experimental constructions of self-dual codes.* in « Finite Fields and Applications », number 3, volume 9, 2003, pages 372-394.

[22] A. KLAPPER, C. CARLET. *Spectral Methods for Cross-Correlations of Geometric Sequences.* in « IEEE Trans. Inform. Theory », 2003, to appear.

[23] P. MILMAN, H. OLLIVIER, J. M. RAIMOND. *Universal quantum cloning in cavity QED.* in « Phys. Rev. A », volume 67, 2003, pages 12314, http://www.arxiv.org/abs/quant-ph/0207039, Also arXiv, quant-ph 0207039.

[24] P. MILMAN, H. OLLIVIER, Y. YAMAGUCHI, M. BRUNE, J.-M. RAIMOND, S. HAROCHE. *Simple quantum information algorithms in cavity QED.* in « J. Mod. Opt. », number 6-7, volume 50, 2003, pages 901-913.

[25] C. S. NEDELOAIA. *Weight Distributions of Cyclic Self-Dual Codes.* in « IEEE Trans. Inform. Theory », number 6, volume 49, June, 2003, pages 1582-1591.

[26] H. OLLIVIER, P. MILMAN. *Proposal for realization of a Toffoli gate via cavity-assisted collision.* in « Quant. Info. Comput. J. », volume 6, 2003, http://www.arxiv.org/abs/quant-ph/0306064, Also arXiv, quant-ph 0306064.

[27] H. OLLIVIER, D. POULIN, W. H. ZUREK. *Emergence of objective properties from subjective quantum states: Environment as a witness.* in « arXiv », number 0307229, volume quant-ph, 2003, http://www.arxiv.org/abs/quant-ph/0307229.

[28] H. OLLIVIER, J.-P. TILLICH. *Description of a quantum convolutional code.* in « Phys. Rev. Lett. », 2003, http://www.arxiv.org/abs/quant-ph/0304189, to appear. Also arXiv, quant-ph 0304189.

[29] D. POULIN, R. BLUME-KOHOUT, R. LAFLAMME, H. OLLIVIER. *Exponential speed-up with a single bit of quantum information: Testing the quantum butterfly effect.* in « arXiv », volume quant-ph, 2003, pages 0310038, http://www.arxiv.org/abs/quant-ph/0310038.

[30] A. SEZNEC, N. SENDRIER. *HAVEGE: User-level Software Heuristic for Strong Random Numbers.* in « ACM Transactions on Modeling and Computer Simulation », number 4, volume 14, October, 2003.

Publications in Conferences and Workshops

[31] D. AUGOT, M. BARDET, J.-C. FAUGÈRE. *Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Groebner bases.* in « Proc. IEEE International Symposium on Information Theory 2003 (ISIT, June 29 - July 4, Yokohama, Japan) », pages 362, 2003.

[32] D. AUGOT, M. FINIASZ. *A public key encryption scheme based on the polynomial reconstruction problem.* in « Advances in Cryptology - EUROCRYPT 2003 », series Lecture Notes in Computer Science, number 2656, Springer-Verlag, pages 229-241, 2003.

[33] A. CANTEAUT, M. DAUM, G. LEANDER, H. DOBBERTIN. *Normal and Non Normal Bent Functions.* in « Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003) », pages 91-100, March, 2003.

[34] C. CARLET. *On the algebraic thickness and non-normality of Boolean functions.* in « Proceedings 2003 IEEE Information Theory Workshop », pages 147-150, Paris, France, March, 2003.

[35] C. CARLET, A. GOUGET. *An upper bound on the number of m-resilient Boolean functions.* in « Advances in Cryptology - Asiacrypt 2002 », series Lecture Notes in Computer Science, volume 2501, Springer-Verlag, pages 484-496, 2003.

[36] C. CARLET, E. PROUFF. *On a new notion of nonlinearity relevant to multi-output pseudo-random generators.* in « Selected Areas in Cryptography, SAC 2003 », series Lecture Notes in Computer Science, Springer-Verlag, 2003, to appear.

[37] C. CARLET, E. PROUFF. *On plateaued Boolean functions and their constructions.* in « Fast Software Encryption, FSE 2003 », series Lecture Notes in Computer Science, Springer-Verlag, 2003, to appear.

[38] C. CARLET, E. PROUFF. *Vectorial Functions and Covering Sequences.* in « Finite Fields and Applications, Fq7 », 2003, to appear.

[39] P. CHARPIN, E. PASALIC. *On propagation characteristics of resilient functions.* in « Selected Areas in Cryptography, SAC 2002 », series Lecture Notes in Computer Science, volume 2595, Springer-Verlag, pages 356–365, 2003.

[40] M. FINIASZ. *Words of minimal weight and weight distribution of binary Goppa codes.* in « Proc. IEEE International Symposium on Information Theory 2003 (ISIT, June 29 - July 4, Yokohama, Japan) », pages 70, 2003.

[41] F. GALAND. *On the Minimum Distance of Some Families of $\mathbf{Z}_{2^k}$-Linear Codes.* in « Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-15 », volume 2643, Springer-Verlag Heidelberg, pages 235 - 243, Toulouse, France, may, 2003.

[42] F. GALAND, G. KABATIANSKY. *Information Hiding by Coverings.* in « Proc. IEEE International Symposium on Information Theory 2003 », Paris, France, March, 2003.

[43] F. GALAND, G. KABATIANSKY. *Steganography via Covering Codes.* in « Proc. IEEE International Symposium on Information Theory 2003, ISIT 03 », Yokohama, Japan, June, 2003.

[44] F. LEVY-DIT-VEHEL, L. PERRET. *A Polly Cracker system secure against linear algebra attacks.* in « Proceedings of the Coding, Cryptography and Combinatorics Conference », Yellow Moutain, China, June, 2003.

[45] F. LEVY-DIT-VEHEL, L. PERRET. *Polynomial equivalence problems and applications to multivariate cryptosystems.* in « Advances in Cryptology - INDOCRYPT 2003 », series Lecture Notes in Computer Science, Springer-Verlag, 2003, to appear.

[46] E. PASALIC. *Degree optimized resilient Boolean functions from Maiorana-McFarland class.* in « Proc. of IMA conference on Coding and Cryptography », Springer-verlag, December, 2003, to appear.

Internal Reports

[47] M. BARDET, J.-C. FAUGÈRE, B. SALVY. *Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over GF(2) with solutions in GF(2).* Technical report, number RR-5049, Rapport de Recherche INRIA, Décembre, 2003, http://www.inria.fr/rrrt/rr-5049.html.

[48] R. BHASKAR. *Group Key Agreement in Ad hoc Networks.* Technical report, number RR-4832, Rapport de Recherche INRIA, December, 2003, http://www.inria.fr/rrrt/rr-4832.html.

[49] F. LEVY-DIT-VEHEL, L. PERRET. *A Polly Cracker system based on satisfiability.* Rapport de recherche, number RR-4698, INRIA, January, 2003.

Miscellaneous

[50] D. AUGOT, M. FINIASZ, P. LOIDREAU. *Using the Trace Operator to repair the Polynomial Reconstruction based Cryptosystem, presented at Eurocrypt 2003.* Cryptology ePrint Archive, Report 2003/209, 2003, http://eprint.iacr.org.

[51] M. CLUZEAU. *Reconstruction d'un brasseur linéaire.* Rapport de stage de DEA, Faculté des Sciences de Limoges, July, 2003.

[52] J. FRIEDMAN, J. TILLICH. *Generalized Alon-Boppana Theorems and Error-Correcting Codes.* 2003, soumis au SIAM Journal of Discrete Mathematics.

[53] P. LOIDREAU. *On the decoding of Maximum Rank Distance codes.* Novembre, 2003, Conférence franco-russe "Mathematics of Communication", Moscou.

[54] T. ROETYNCK. *Implémentation d'un cryptosystème basé sur les codes correcteurs d'erreurs.* Rapport de stage ingénieur, ENSTB, September, 2003.

[55] N. SENDRIER. *Encoding information into constant weight words.* submitted, 2003.

[56] N. SENDRIER. *Linear Codes with Complementary Duals Meet the Gilbert-Varshamov Bound.* submitted, 2003.