INRIA

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]
Matthieu Finiasz [post-doctorant à l'EPFL, Lausanne, Suisse]
Philippe Gaborit [Université Limoges]
Grigory Kabatiansky [IPIT, Académie des Sciences de Moscou, Russie]
Françoise Levy-dit-Vehel [ENSTA]
Pierre Loidreau [ENSTA]
Carmen Nedeloaia [ATER, Université Paris 8]
Harold Ollivier [post-doctorant au Perimeter Institute, Waterloo, Canada]

Ingénieur expert
Fabien Galand

Post-doctorants
Avishek Adhikari
Marine Minier
Michaël Quisquater

Doctorants
Raghav Bhaskar [Bourse Égide]
Thomas Camara [Bourse MESR]
Mathieu Cluzeau [Bourse DGA]
Frédéric Didier [Normalien]
Cédric Faure [Normalien]
Yann Laigle-Chapuy [AMN]
Cédric Lauradoux [Bourse INRIA]
Ludovic Perret [Bourse MESR]
Andrea Roeck [Bourse INRIA]
Bassem Sakkour [Bourse syrienne]
Marion Videau [Bourse DGA]

Stagiaires
Youssef Ridene [stage 1ère année d'IUP GMI, Université de Paris 8, de juillet 2005 à août 2005]
Stéphane Manuel [stage de maîtrise, Université de Paris 8, de janvier 2005 à septembre 2005]
Domitille Heitzler [stage de maîtrise, Université de Cergy Pontoise, d'avril 2005 à juin 2005]

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. Duaux des codes BCH

Participant: Carmen Nedeloaia.

Carmen Nedeloaia a continué l'étude des duaux des codes BCH dans [90]. La construction carrée modifiée des codes affines-invariants introduite 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 étaient connues auparavant. Ils ont également été vérifiés par l'algorithme Canteaut-Chabaud de recherche de mots de petits poids dans un code.

4.1.2. Recherche de mots de poids faible dans un code

Participants: Carmen Nedeloaia, Philippe Gaborit.

Un travail en commun avec Philippe Gaborit (Université de Limoges) et Alfred Wassermann (Université de Bayreuth-Allemagne) a été mené autour d'un algorithme de calcul de mots de poids donné 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 à A.

[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.

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. Ces travaux ont donné lieu à la publication [36].

4.1.3. 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 ont 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.

Pierre 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.

4.2. Cryptographie à clé publique

4.2.1. Système de chiffrement utilisant des codes correcteurs

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

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, Stéphane Manuel, 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".

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 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'étude de méthodes de cryptanalyse de schémas à clef publique multivariés s'est poursuivie par l'optimisation des algorithmes précédemment trouvés, ou la recherche de meilleurs algorithmes. Ainsi, Ludovic Perret a présenté à la conférence Eurocrypt'05 [80] un nouvel algorithme permettant de résoudre le problème de l'isomorphisme de polynômes à un secret. Cette méthode utilise une caractérisation différentielle de ce problème permettant d'obtenir des équations linéaires en les composantes d'une matrice solution. Elle constitue un premier pas vers la cryptanalyse de systèmes cryptographiques tels que C^* ou SFLASH. La puissance de résolution pratique de systèmes multivariés sur des corps finis par les algorithmes F4 ou F5 conduit actuellement Ludovic Perret et Françoise Levy-dit-Vehel à considérer cette approche sur d'autres problèmes de cryptographie multivariée.

Dans le cadre de la cryptanalyse de systèmes fondés sur le problème du mot, Françoise Levy-dit-Vehel et Ludovic Perret ont orienté leur travail selon deux approches: dans la première, ils exploitent des propriétés des monoïdes partiellement commutatifs pour retrouver la clef secrète d'un tel système (le schéma de chiffrement de Wagner-Magyarik, publié à Crypto'84); la deuxième utilise une attaque à chiffré choisi pour cryptanalyser un système reposant sur les mots de Lyndon (le schéma de chiffrement de Siromoney-Matthew, paru dans IP Letters'90). Deux articles sur ce sujet ont été présentés à la conférence WCC'05 [79], [75].

4.2.5. Cryptosystèmes fondés sur des problèmes algébriques

Participants: Daniel Augot, 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. 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 de 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. C'est une généralisation non triviale, on peut même dire qu'il n'y a pas de généralisation naturelle. Ainsi de nombreuses propositions ont été faites, plus ou moins performantes en termes soit de calcul, soit de communications. Daniel Augot et Raghav Bhaskar ont proposé une variante du protocole de Diffie-Hellman, qui s'étend bien au contexte multi-utilisateurs. Raghav Bhaskar a établi une preuve de sécurité de ce protocole, ce qui, théoriquement, le met à l'abri de toute attaque éventuelle.

Bien que ce protocole ne soit pas le plus performant en termes de répartition des calculs (un des particpants doit accepter une charge de calcul en $O(n)$ où n est le nombre de participants), il est celui qui requiert le moins d'organisation entre les participants. C'est un net progrès par rapport à l'existant, car les protocoles les plus performants exigent une organisation tantôt en ronde, tantôt en arbre, des participants. En pratique, ces protocoles ne sont pas très raisonnables. Le protocole a été publié à la conférence Workshop on Trust, Security and Privacy in Ubiquitous Computing.

Ce protocole semble donc bien adapté pour être utilisé dans le contexte des réseaux ad hoc. Daniel Augot et Raghav Bhaskar sont en discussion avec Hipercom (Paul Mühlethaler), pour définir les modalités d'utilisation pratique de ce protocole de mise en accord de clé. Ce travail s'inscrit aussi dans le cadre de l'ACI SERAC.

4.3. Algorithmes de décodage

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, dont les performances exceptionnelles ont révolutionné les codes correcteurs.

4.3.1. Décodage itératif

Participant: Jean-Pierre Tillich.

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. Ces travaux ont conduit Jean-Pierre Tillich, en collaboration avec Iryna Andriyanova et Jean-Claude Carlach, à optimiser les paramètres de cette amélioration des codes LDPC. Ils obtiennent ainsi des codes binaires qui se placent parmi les meilleurs connus pour des taux d'erreur bloc faibles (c'est à dire inférieurs à 10^{-5}) et une large gamme de rendement comprise entre $1/2$ et $1/10$. Une partie de ces travaux a été publiée dans [42], [43].

4.3.2. Codes de Reed-Muller

Participants: Frédéric Didier, Pierre Loidreau, Bassem Sakkour, Jean-Pierre Tillich.

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.

Frédéric Didier et Jean-Pierre Tillich, s'intéressent à ces mêmes codes, mais pour un modèle d'erreur qui est le canal à effacement. L'intérêt de ce modèle d'erreur vient du fait que si l'on est capable de décoder efficacement des codes de Reed-Muller pour ce canal, alors cela fournit également un algorithme efficace de calcul de l'immunité algébrique de fonctions booléennes. Rappelons que ce paramètre quantifie l'immunité d'une fonction booléene cryptographique vis à vis des attaques algébriques. Frédéric Didier a commencé une étude fondamentale de la probabilité de ne pas arriver à compenser les effacements d'un code pour le canal à effacement. Il a notamment obtenu une borne supérieure sur cette probabilité qui peut être appliquée aux codes de Reed-Muller. Cette borne explique entre autres pourquoi l'immunité algébrique d'une fonction booléene aléatoire est aussi élevée. Ce travail va être publié dans [25].

Frédéric Didier et Jean-Pierre Tillich ont utilisé cette borne pour analyser un algorithme de décodage de codes de Reed-Muller sur le canal à effacements. Cela leur a permis de montrer que ce décodage avait, pour un ordre fixé, une complexité linéaire. Ceci améliore de manière notable les meilleurs algorithmes connus, et permet de calculer l'immunité algébrique de fonctions booléennes jusqu'à des ordres assez elevés et pour un grand nombre de variables [92].

4.3.3. Décodage fondé sur l'interpolation

Participant: Daniel Augot.

Daniel Augot a travaillé sur les algorithmes de décodage basés sur l'interpolation dérivés de l'algorithme de Sudan et de Guruswami-Sudan. Le premier axe est d'essayer d'améliorer la complexité de ces algorithmes qui reste grande. C'est un travail en cours avec Jean-Charles Faugère, car les techniques de base de Gröbner sont bien appropriées pour implanter diverses étapes de l'algorithme. De manière plus générale, le calcul formel est plus avancé que les techniques de décodage pour traiter efficacement la mise en œuvre des algorithmes à base d'interpolation.

L'autre axe de recherche est de généraliser le contexte d'application des techniques à base d'interpolation à d'autres codes. Avec Mikhail Stepanov de l'université de Saint Petersburg, Daniel Augot a proposé une généralisation naturelle, mais non triviale, aux cas multivariés, c'est-à-dire aux codes produit de Reed-Solomon et aux codes de Reed-Muller généraux. Les résultats en terme de performance ne sont pas ceux espérés, et il semble maintenant qu'il faille devoir utiliser des techniques plus spécifiques, que simplement la généralisation à plusieurs variables. Il est envisagé, dans les perspectives, de s'intéresser à l'application des algorithmes à base d'interpolation aux codes concaténés.

4.3.4. Décodage des codes cycliques avec les bases de Gröbner

Participant: Daniel Augot.

Par ailleurs, en collaboration avec Magali Bardet et Jean-Charles Faugère, Daniel Augot s'intéresse également au décodage des codes cycliques avec les bases de Gröbner. Il s'agit de décoder des codes cycliques *génériques* qui n'ont pas a priori d'algorithmes de décodage, comme par exemple les codes à résidus quadratiques. Bien qu'en pratique les résultats indiquent la validité de la méthode, nous essayons de démontrer les bonnes propriétés des algorithmes de décodage fondés sur les bases de Gröbner.

4.4. Reconnaissance de codes

Participants: Anne Canteaut, Mathieu Cluzeau, Nicolas Sendrier, Jean-Pierre Tillich.

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. Fonctions booléennes

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*.

4.5.1. Propriétés cryptographiques des fonctions booléennes

Participants: Claude Carlet, Pascale Charpin, Philippe Gaborit.

Les primitives de chiffrement symétrique font largement appel aux fonctions booléennes, et leur sécurité dépend de manière essentielle des propriétés cryptographiques de ces dernières. La recherche consiste ici à la fois à étudier les propriétés cryptographiques de fonctions booléenes impliquées dans des schémas existants et à proposer de nouvelles fonctions booléennes ayant de bonnes propriétés cryptographiques.

Ainsi, Claude Carlet a introduit et étudié une construction de fonctions cryptographiques basée sur la concaténation (selon le même principe que pour les fonctions de Maiorana-McFarland) de sommes d'indicatrices d'espaces affines et de fonctions affines [12]. En collaboration avec J. Yucas, il a introduit plusieurs constructions secondaires de fonctions booléennes courbes ayant la particularité de générer des fonctions de n variables à partir de fonctions de n variables, tout en en augmentant le degré. Cela a en particulier mené à l'introduction de larges classes de fonctions de degré 3, construites à partir de fonctions quadratiques [19]. Avec S. Maitra et S. Gangopadhyay, il a montré que les fonctions PSap de Dillon ont des corrélations croisées à 3 valeurs et que le nombre de valeurs monte à au plus 5 pour des fonctions définies suivant le même principe mais non nécessairement courbes [63].

En collaboration avec H. Dobbertin, G. Leander, A. Canteaut, P. Felke et P. Gaborit, il a introduit diverses classes de fonctions courbes dont les représentations traces comportent deux monômes [10]. En collaboration avec P. Gaborit, il a poursuivi l'étude, faite par A. M. Youssef et G. Gong, des fonctions dites "hyper-courbes". Il a montré que ces fonctions appartiennent toutes à un certain code cyclique étendu et en a déduit, d'une part que leur degré est toujours égal à $n/2$, et d'autre part que, pour une infinité de valeurs du nombre n de variables, elles sont à une équivalence près, égales aux fonctions PSap de J. Dillon [18]

Avec le même collègue, il a mené une étude du récent critère cryptographique d'immunité algébrique qui quantifie la résistance des fonctions booléennes aux attaques algébriques classiques [62]. Il ressort de cette étude que les fonctions aléatoires sont d'immunité algébrique élevée et que les attaques algébriques ont été si efficaces, sur plusieurs schémas cryptographiques à la volée connus, du fait que les fonctions booléennes impliquées dans ces schémas soit avaient trop peu de variables soit avaient été choisies de façon trop particulière. Un travail équivalent sur les attaques algébriques rapides est en cours.

Pascale Charpin s'intéresse-elle à la classification des fonctions booéennes résilientes, (voir [14]). La résilience est un critère de non-corrélations éxigé surtout dans les sytèmes de chiffrement par flot. Claude Carlet et Pascale Charpin ont continué leur travaux dans ce domaine en décrivant complètement les fonctions de degree 3 et de meilleur résilience. Comme l'on pouvait s'y attendre, ils ont aussi montré que leur propriétés cryptographiques sont globalement mauvaises.

Une technique courante pour construire de larges classes de fonctions booléennes ayant de bonnes propriétés cryptographiques est de partir d'une fonction simple répondant à un certain nombre de ces critères et d'en déduire d'autres. Par exemple, Pascale Charpin [24], à la suite d'une suite d'articles dus principalement à l'équipe de Waterloo (Guang Gong), cherche à construire, à partir de fonctions quadratiques, de *bonnes* fonctions Booléennes de degré supérieur. Sa contribution s'inscrit dans les deux principaux aspects : caractériser des classes de fonctions quadratiques hautement linéaires et exhiber des propriétés applicables en concaténation.

4.5.2. Fonctions booléennes symétriques

Participants: Anne Canteaut, Marion Videau.

Anne Canteaut et Marion Videau s'attachent elles à étudier les propriétés cryptographiques des fonctions 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. Une étude détaillée des propriétés des fonctions symétriques de degré inférieur ou égal à 8 a également été menée. Elle a permis d'obtenir la liste de toutes les fonctions symétriques équilibrées à n variables de degré inférieur à 8. L'article a été publié dans la revue IEEE-IT [11]. Suite à ce travail, Marion Videau s'est attachée à caractériser les fonctions symétriques de non-linéarité élevée. Ce résultat a enrichi la publication à IEEE-IT [11] et a également fait l'objet de d'une communication à WEWoRC 2005 [85]. Elle a également commencé à étudier avec Matthew Parker, pendant son séjour à Bergen, les propriétés des fonctions booléennes symétriques relativement à d'autres transformations que la transformée de Walsh. Elle a par ailleurs entamé l'étude de la propriété d'immunité algébrique des fonctions booléennes symétriques avec An Braeken.

4.5.3. Fonctions vectorielles

Participants: Claude Carlet, Pascale Charpin.

Dans cet axe de recherche, le projet s'intéresse aux propriétés cryptographiques de généralisations multidimensionnelles (voir sur d'autres corps que le corps à deux éléments) des fonctions booléennes.

Par exemple, Claude Carlet avec L. Budaghyan et A. Pott, a exploité la notion d'équivalence des fonctions vectorielles introduite dans l'article "Codes, bent functions and permutations suitable for DES-like cryptosystems" de P. Charpin, V. Zinoviev et lui-même, pour en déduire de nouvelles fonctions presque parfaitement non-linéaires ou presque courbes, qui sont non affinement équivalentes aux fonctions connues et qui sont même non affinement équivalentes aux fonctions puissances dans les corps finis [54]. C. Carlet a ensuite généralisé ces constructions grâce à l'observation d'une propriété très simple, mais jamais observée, des fonctions booléennes. Celle-ci lui a permis d'obtenir une construction secondaire générale de fonctions courbes et

également une construction similaire de fonctions résilientes de haute nonlinéarité, qui a en outre la propriété d'augmenter l'immunité algébrique des fonctions [61], [13].

En collaboration avec C. Ding, il a introduit une nouvelle approche de la nonlinéarité des fonctions vectorielles (les boîtes S des systèmes de chiffrement par blocs), et il a obtenu trois nouvelles bornes supérieures qui améliorent à la fois la borne liée au rayon de recouvrement du code de Reed-Muller d'ordre 1 et celle de Sidelnikov (redécouverte par Chabaud et Vaudenay), chacune pour des ordres de grandeurs différents du rapport n/m du nombre de bits de sortie de la fonction sur le nombre de bits d'entrée [15]. Parallèlement, il a montré le mauvais comportement des fonctions vectorielles hautement non-linéaires connues (en particulier la fonction inverse, utilisée comme boîte S dans l'AES) vis à vis du nouveau paramètre introduit par E. Prouff au congrès FSE 2005, lié à l'aptitude de ces fonctions à déjouer les attaques DPA (differential power analyses) et à éviter ainsi des contre-mesures coûteuses en temps et en capacité de stockage dans les cartes à puces [61].

Pascale Charpin en collaboration avec Enes Pasalic [23], a trouvé une construction de fonctions vectorielles ayant de bonnes propriétés cryptographiques en utilisant 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.

4.5.4. Lien entre fonctions booléennes et codes correcteurs

Participants: Claude Carlet, Pascale Charpin.

De nombreux liens existent entre les propriétés cryptographiques des fonctions booléennes ou vectorielles et la théorie des codes correcteurs d'erreurs. Par exemple, Claude Carlet en collaboration avec C. Ding et J. Yuan, a introduit certains codes optimaux ou sous-optimaux, construits à partir de fonctions hautement non-linéaires, et il en a déduit des schémas de partage du secret, dont les performances sont parmi les meilleures connues [17]. Il a poursuivi ce travail en déterminant la distribution des poids de divers codes linéaires liés à des fonctions vectorielles hautement non-linéaires [13]. Il l'a encore prolongé, avec C. Ding et H. Niederreiter, en appliquant les fonctions hautement non-linéaires à la construction de schémas d'authentification dont les performances sont parmi les meilleures connues [16]. En collaboration avec S. Mesnager, il a engagé une étude sur la structure des supports de Walsh des fonctions booléennes et il a amélioré la meilleure borne supérieure connue (datant de 13 ans) sur le rayon de recouvrement des codes de Reed-Muller d'ordres supérieurs à 1 [64].

Pascale Charpin étudie elle les liens qui existent entre certaines fonctions vectorielles, les sommes de Kloosterman et les codes BCH. C'est une recherche qui s'inscrit dans la durée (avec Helleseth et Zinoviev) qui porte globalement sur les liens entre sommes exponentielles et translatés de codes. S'agissant des BCH 3-correcteurs, apparaissent les sommes cubiques, leurs inverses et les sommes de Kloosterman (voir [20]). Kloosterman, c'est la fameuse fonction $x \mapsto x^{-1}$. Les propriétés de propagation de cette fonction inverse apparaissent dans les calculs sur les translatés de poids 4 et ceci est repris dans un article séparé (voir [21]).

Enfin cette étude en profondeur a amené ces mêmes auteurs à démontrer et compléter la vieille conjecture de Horst et Berger (1976) en déterminant la distribution des translatés des codes correcteurs (voir [22], [65]).

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

Participants: Daniel Augot, Thierry Berger, Anne Canteaut, Pascale Charpin, Cédric Lauradoux, Marine Minier, Nicolas Sendrier, Marion Videau.

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.

Dans le cadre de l'appel à soumission du réseau d'excellence européen ECRYPT (on peut trouver la documentation concernant ce réseau sur http://www.ecrypt.eu.org/), Anne Canteaut, Cédric Lauradoux et Marine Minier (en collaboration avec des chercheurs de France Télécom et de l'ENS) ont soumis deux nouveaux algorithmes de chiffrement à flot, le premier SOSEMANUK [50] est dédié au software tandis que le deuxième DECIM [49] est orienté hardware.

Thierry Berger, Cédric Lauradoux et François Arnault ont quant à eux travaillé à la mise au point et à la cryptanalyse d'une famille de systèmes de chiffrement à flot fondée sur un circuit FCSR filtré (F-FCSR). Ce générateur a été proposé à l'appel à proposition ECRYPT sur les Stream Ciphers. Il est fondé sur un automate de division 2-adique (Feedback with Carry Shift Register) et un filtre linéaire sur les cellules de l'automate. Ce générateur est en cours d'évaluation. Une cryptanalyse algébrique sur un protocole affaibli de changement d'IV a été proposée par Marine Minier et Thierry Berger [52].

4.7. Chiffrement symétrique : cryptanalyse

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

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.

4.7.3. Attaques sur les canaux auxiliaires et micro-architecture

Participants: Anne Canteaut, Cédric Lauradoux.

L'implémentation d'un algorithme de chiffrement est une question délicate. En effet, les grandeurs physiques associées à l'implémentation (comme le temps ou la consommation de puissance) peuvent donner de l'information à l'attaquant quand à la clef secrète employée. Dans ce contexte, Anne Canteaut et Cédric Lauradoux se sont intéressés avec le concours d'André Seznec aux attaques relatives à la micro-architecture et plus particulièrement aux mémoires caches. Les mémoires caches peuvent provoquer d'importantes variations sur le temps de calcul ou sur la consommation de puissance. De plus, même si l'on élimine l'influence des caches, la micro-architecture des processeurs modernes influence significativement le temps de calcul. Nous avons pu étudier toutes ces attaques contre l'AES et proposer des contre mesures adéquates.

4.8. Génération logicielle de nombres aléatoires par l'entropie intrinsèque aux calculateurs

Participants: Andréa Röck, 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.

4.9. Sécurité informatique et sécurité juridique

Participants: Anne Canteaut, Marion Videau.

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.

4.10. 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. Des résultats partiels ont été obtenus dans ce sens, et ont donné lieu aux publications [55], [78].

5. Contracts and Grants with Industry

5.1. Contracts and Grants with Industry

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

5.1.1. 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. 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.

6.1.1.2. 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.

6.1.1.3. ACI OCAM

de septembre 2003 à aoôut 2006, dont le but est d'étudier l'implantation matérielle de primitives cryptographiques utilisant la théorie algébrique des codes. Plus particulièrement, nous nous proposons de mettre en oeuvre en FPGA le système de signature proposé par Courtois, Finiasz et Sendrier à Asiacrypt 2001.

6.1.1.4. ACI UNIHAVEGE

de septembre 2003 à aoôut 2006, dont l'ambition est de montrer que l'approche logicielle du générateur de nombres aléatoire HAVEGE est une approche "universelle" et facilement portable pour générer de l'aléa irreproductible sur toute la gamme des systèmes informatiques communicants bâtis autour des microprocesseurs hautes performances.

6.1.1.5. 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.

6.1.1.6. 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.

6.1.1.7. 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).

6.1.1.8. ACI SERAC

de septembre 2004 à Août 2007, "models and protocols for *SE*cuRity in wireless Ad hoC networks". L'axe de recherche principal est de "sécuriser" le routage dans les réseaux ad hoc, l'accent étant mis sur OLSR, grâce à la présence d'Hipercom dans le projet. Les différentes menaces ont été identifiées. Pour l'instant les solutions recherchées sont de nature cryptographique. Il est envisagé de développer d'autres modèles pour étudier les attaques sur un réseau ad hoc sans fil. Caroline Fontaine est la coordinatrice du projet qui regroupe les partenaires suivants : USTL, INRIA (projet Codes, Tanc et Hipercom) et le GET.

6.1.1.9. RNRT X-CRYPT

Le RNRT X-CRYPT (avec Schlumberger, École normale supérieure, France Telecom, Cryptolog International, Université de Versailles) a été labellisé en 2003 (3 ans). Anne Canteaut est responsable du groupe "chiffrement à flot rapide".Dans le cadre de ce contrat, le projet CODES (A. Canteaut, M. Minier et C. Lauradoux) a participé à la conception de trois nouveaux systèmes de chiffrement à flot soumis en avril 2004 en réponse à l'appel lancé par le Réseau d'Excellence européen ECRYPT (voir http://www.ecrypt.eu.org/stream/).

6.1.1.10. 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". Dans ce cadre, elle est l'éditeur d'un rapport intitulé *Open Research Areas in Symmetric Cryptography and Technical Trends in Lightweight Cryptography*.

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[3] depuis octobre 99.

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

6.1.3. Participations à des instances et manifestations nationales

Plusieurs membres du projet participent à des commissions de spécialistes :

Université de 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.

Thierry Berger est membre du Comité Scientifique des journées Codes-Cryptographie d'Aussois.

Pascale Charpin est membre du comité scientifique de l'Action Concertée Incitative (ACI) "Sécurité et Informatique", 2002-06 et membre du comité scientifique STICs pour les Appels à Projets Non Thématiques (ANT et ANJ) de l'Agence nationale de la recherche.

A. Canteaut est membre du groupe de travail "Conservation électronique des documents" du Forum des Droits sur l'Internet, qui a publié une recommandation sur le sujet fin novembre 2005. Elle est aussi présidente du Comité des Bourses de l'INRIA Rocquencourt.

C. Carlet est responsable de l'équipe d'accueil MAATICAH (Mathématiques et Algorithmique Appliquées aux Technologies de l'Information et de la Communication, Approche Historique) de l'Université Paris 8 et responsable du groupe de travail "Codage et Cryptographie" (C2) du GDR ALP, devenu le GDR IM (Informatique mathematique).

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 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 *International Workshop on Coding and Cryptography* et a la responsabilité des soumissions electroniques à ce colloque.
- Anne Canteaut est membre des comités de programme de FSE 2005, BeNeLuxFra Conference in Mathematics, WCC2005, SKEW (Symmetric Key Encryption Workshop), WEWoRC, FSE 2006, SASC 2006 (où elle est Program chair) et SETA 06.
- Claude Carlet est membre des comités de programme de BFCA *First Workshop on Boolean Functions : Cryptography and Applications*, Rouen, Mars 2005; de WCC2005, SETA 06, Pékin, Septembre 24-28, 2006; YACC *Yet Another Conference on Cryptography*, Ile de Porquerolles, 2006.
- Pascale Charpin est co-présidente du comité de programme de WCC2005 (co-présidence avec O. Ytrehus), Mars 2005, Bergen, Norvège.
- Françoise Lévy-dit-Véhel est membre du comité d'organisation de FSE 2005 et du comité de programme d'Indocrypt 2005, Bangalore, Inde.
- Nicolas Sendrier est membre du comité de programme WCC2005, WEWoRC 2005, Leuven, Belgique, juillet 2005 et ASIACRYPT 2005, Madras, Inde.

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 :

- A. Canteaut est Associate Editor pour la revue “IEEE Transactions on Information Theory” (spécialité “ Cryptographie et Complexité”).
- 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*, ouvrage paru en 2005; 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

- Bimal ROY (professeur), Indian Statistical Institute, Kolkata, INDE, 13/01/05 au 14/01/05,
- Oyvind YTREHUS (professeur), University of Bergen, NORVÈGE, 27/01/05 au 29/01/05,
- Deepak KUMAR DALAI (étudiant en thèse) , Indian Statistical Institute, Kolkata, INDE, 24/02/05 au 24/03/05,
- Michael QUISQUATER (chercheur postdoctoral) ,Katholieke Universiteit Leuven, Heverlee, BELGIQUE, (28/02/05 au 01/03/05),
- Vladimir SIDELNIKOV (professeur), Lomonosov University, MSU, Moscow, RUSSIE, 03/04/05 au 30/04/05,
- Andrea RÖCK (étudiante en mastère), University of Salzburg, AUTRICHE,25/05/05 au 27/05/05,
- David HACCOUN (professeur) , Ecole Polytechnique de Montreal, Quebec, CANADA, 02/06/05 au 03/06/05,
- Harold OLLIVIER (chercheur postdoctoral), Perimeter Institute for Theoretical Physics, Waterloo, CANADA, 05/07/05 au 12/07/05, 05/09/05 au 19/09/05,
- Gohar KYUREGHYAN (professeur) , University of Magdeburg, Allemagne, 15/09/05 au 14/10/05,
- Mikhail STEPANOV (étudiant en thèse), St Petersburg State University of Aerospace Instrumentation, RUSSIE, 02/10/05 au 16/12/05,
- Grigory KABATIANSKIY (professeur), Institute for Problems of Information Transmission, RAS, Moscow, RUSSIE, 03/04/05 au 30/04/05, 19/09/05 au 23/09/05, 20/11/05 au 16/12/05,
- Mridul NANDI (étudiant en thèse), Indian Statistical Institute, Kolkata, INDE, 15/12/05 au 15/03/06.

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 assure une partie du cours de codes correcteurs d'erreurs dans le MPRI ainsi que le cours de cryptologie dans le mastère informatique de Marne la Vallée.
- Jean-Pierre Tillich intervient également dans le MPRI Algorithmique, filière Traitement et protection de l'Information, pour assurer une partie du cours de codes correcteurs d'erreurs, ainsi qu'un cours de codes correcteurs d'erreurs en dernière année de l'ISEP.
- 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 : Informatique fondamentale (petites classes), 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 :

Février 2005 Carmen Nedeloaia, *Etude des énumérateurs des poids des codes linéaires utilisant des formes décomposées des matrices génératrices*, Université de Limoges, jury :T. Berger, P. Charpin (direction).

Juin 2005 Hatem Hadj Kacem, *Contributions à la théorie et aux applications des automates à multiplicités*, Université de Rouen, jury :C. Carlet (rapporteur).

Juin 2005 Guénaël Renaud, *Calcul efficace de corps de décomposition*, Université Paris 6, jury :P. Charpin.

Août 2005 Havard Molland , *New Methods for Cryptanalysis of Stream Ciphers*, University of Bergen, jury : A. Canteaut (first opponent).

Septembre 2005 Laurent Poinsot, *Non linéarité parfaite généralisée au sens des actions de groupe, contribution aux fondements de la solidité cryptographique*, Université de Toulon, jury : A. Canteaut (présidente).

Danièle Raffo, *Security Schemes for the OLSR Protocol for Ad Hoc Networks*, Université Paris 6, jury :D. Augot.

Octobre 2005 Laurent Dubreuil, *Amélioration de l' étalement de spectre par l'utilisation de codes correcteurs d'erreurs*, Université de Limoges, jury :T. Berger (direction), N. Sendrier (rapporteur).

Ludovic Perret, *Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique*, Université de Marne-la-Vallée, jury :F. Levy-dit-Vehel.

Novembre 2005 Samuel Maffre, *Conjugaison et cyclage dans les groupes de Garside, applications cryptographiques*, Université de Limoges, jury :T. Berger (direction), P. Gaborit.

Marion Videau, *Critères de sécurité des algorithmes de chiffrement à clé secrète*, Université Paris 6, jury : A. Canteaut (direction) et P Charpin (co-direction).

7.3. Participation à des colloques

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

Séjours courts dans des universités ou laboratoires en 2005 :

- Collaboration avec Los Alamos National Laboratory et l'université de Californie. Harold Ollivier y a été invité à plusieurs reprises.
- Collaboration avec le Perimeter Institute Canada. Jean-Pierre Tillich y a été invité deux semaines en novembre.
- Collaboration avec l'Université de Bergen (Norvège), Marion Videau a été invité pendant 6 mois, Pascale Charpin y a passé quelques semaines et Anne Canteaut quelques jours.
- Collaboration avec l'ISI Calcutta, Asiacrypt, Indocrypt, Bangalore, Nicolas Sendrier y a été invité une semaine en décembre par Bimal Roy.
- Collaboration avec l'Université de St-Petersburg, Russie. Frédéric Didier, Pierre Loidreau, Jean-Pierre Tillich et Marion Videau ont été invités en mai 2005, dans le cadre du programme ECONET de collaboration Bulgarie-Russie-France (géré par P. Loidreau).

Participations aux colloques en 2005 :

- QIP Cambridge, Boston, 12/01 au 18/01/05, participants : Thomas Camara, Harold Ollivier.
- Journées C2, Aussois, 30/01 au 04/02/05, participants : Raghav Bhaskar, Claude Carlet, Pascale Charpin, Cédric Faure, Fabien Galand, Yann Laigle-Chapuy, Marine Minier, Jean-Pierre Tillich.
- WCC, Bergen, 13/03 au 18/03/05, participants : Daniel Augot, Anne Canteaut, Claude Carlet, Pascale Charpin, Cédric Faure, Françoise Lévy-dit-Véhel, Ludovic Perret, Nicolas Sendrier, Vitaly Shorin.
- Ecole Jeunes Chercheurs d'algorithmique Montpellier, 03/04 au 08/04/05, participants : Anne Canteaut, Mathieu Cluzeau, Frédéric Didier, Cédric Lauradoux.
- Ecrypt Summer School on Cryptanalysis, Samos, 09/05 au 14/05/05, participants : Yann Laigle-Chapuy, Nicolas Sendrier.
- EUROCRYPT, Aarhus, 22/05 au 26/05/05, participants : Anne Canteaut, Cédric Lauradoux.
- ECRYPT SVTL, Aarhus, 26/05 au 27/05/05, participants : Anne Canteaut, Cédric Lauradoux.
- Joint BeNeLuxFra Conference in Mathematics, Gand, 20/05 au 21/05/05, participants : Daniel Augot, Magali Bardet, Anne Canteaut.
- Coding Theory Days and MIPT and Bauman University, 18/05 au 01/06/05, participant : Vitaly Shorin.
- Colloque, Caen, 30/05 au 31/05/05, participant : Nicolas Sendrier.
- ING 2005 Montreuil/Mer, 13/06 au 17/06/05, participants : Daniel Augot, Cédric Lauradoux.
- 4th Analogue decoding workshop, Rennes, 15/06 au 17/06/05, participant : Jean-Pierre Tillich.
- ECRYPT, Cracovie, 22/06 au 26/06/05, participants : Stéphane Manuel, Nicolas Sendrier.
- Réunion Réseau Européen, Leuven, 29/06 au 01/07/05, participant : Anne Canteaut.
- WEWoRC 2005, Leuven-Heverlee, 05/07 au 07/07/05, participants : Fabien Galand, Cédric Lauradoux, Marine Minier, Nicolas Sendrier, Marion Videau.
- 8th ISCTA, Ambleside, UK, 16/07 au 23/07/05, participant : Vitaly Shorin.
- Réunion de travail chiffrement à flot, Bergen, 09/08 au 12/08/05, participant : Anne Canteaut.

- Crypto, Santa Barbara, du 13/08 au 19/08/05, participant : Raghav Bhaskar.
- EQIS, Tokyo, Japon, 25/08 au 03/09/05, participant : Thomas Camara.
- ISIT, Adelaide, 02/09 au 16/09/05, participants : Claude Carlet, Yann Laigle-Chapuy, Pierre Loidreau, Nicolas Sendrier, Jean-Pierre Tillich.
- Conférence AGCT, Marseille, 26/09 au 30/09/05, participant : Daniel Augot.
- IEEE Information Theory Workshop, Awaji Island, Japon, 14/10 au 20/10/05, participant : Anne Canteaut.
- PaRISTIC, Bordeaux, 21/11 au 23/11/05, participant : Cédric Lauradoux.
- Journées Quantiques & Co, Lyon, 23/11/05, participant : Thomas Camara.
- Indocrypt, Bangalore, Inde, 07/12 au 13/12/05, participants : Françoise Lévy-dit-Véhel, Claude Carlet.
- Journées COST, Grenoble, 12/12 au 14/12/05, participants : Daniel Augot, Raghav Bhaskar, Cédric Lauradoux.

8. Bibliography

Books and Monographs

[1] E. FILIOL. *Computer viruses: from theory to applications*, vol. ISBN 2-287-23939-1, IRIS International series, Springer Verlag, june 2005.

[2] G. KABATIANSKY, E. KROUK, S. SEMENOV. *Error Correcting Codes and Security for Data Networks*, 278 pages, vol. ISBN 0-470-86754-X, John Willey & Sons Ltd, 2005.

Doctoral dissertations and Habilitation theses

[3] C. S. NEDELOAIA. *Etude des énumérateurs des poids des codes linéaires utilisant des formes décomposées des matrices génératrices*, Thèse de doctorat, Université de Limoges, Février 2005.

[4] L. PERRET. *Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique*, Thèse de doctorat, Université de Marne-la-Vallée, Octobre 2005.

[5] M. VIDEAU. *Critères de sécurité des algorithmes de chiffrement à clé secrète*, Thèse de doctorat, Université Pierre et Marie Curie (Paris 6), Novembre 2005.

Articles in refereed journals and book chapters

[6] F. ARNAULT, T. BERGER. *Design and properties of a new pseudo-random generator based on a filtered FCSR automaton*, in "IEEE, Transactions on Computers", to appear, 2005.

[7] T. BERGER, A. CANTEAUT, P. CHARPIN, Y. LAIGLE-CHAPUY. *On Almost Perfect Nonlinear functions*, in "IEEE Trans. Inform. Theory", To appear, 2005.

[8] T. BERGER, P. LOIDREAU. *How to mask the structure of codes for a cryptographic use*, in "Designs, Codes and Cryptography", vol. 35, april 2005, p. 63-79.

[9] R. BHASKAR, D. AUGOT, V. ISSARNY, D. SACCHETTI. *A Three Round Authenticated Group Key Agreement Protocol for Ad hoc Networks*, in "Elsevier Journal on Pervasive and Mobile Computing", To appear, 2005.

[10] A. CANTEAUT, C. CARLET, H. DOBBERTIN, P. FELKE, P. GABORIT, G. LEANDER. *Construction of bent functions via Niho power functions*, in "Journal of Combinatorial Theory", 2005.

[11] A. CANTEAUT, M. VIDEAU. *Symmetric Boolean functions*, in "IEEE Trans. Inform. Theory", Regular Paper, vol. 51, n° 8, 2005, p. 2791–2811.

[12] C. CARLET. *Concatenating indicators of flats for designing cryptographic functions*, in "Designs, Codes and Cryptography", vol. 36, 2005, p. 189-202.

[13] C. CARLET. *The Weight Distribution of a Class of Linear Codes from Perfect Nonlinear Functions*, in "IEEE Trans. Inform. Theory", to appear, 2005.

[14] C. CARLET, P. CHARPIN. *Cubic Boolean functions with highest resiliency*, in "IEEE Trans. Inform. Theory", Regular paper, vol. 51, n° 2, February 2005, p. 562-571.

[15] C. CARLET, C. DING. *Nonlinearities of S-boxes*, in "Finite Fields and Their Applications", to appear, 2005.

[16] C. CARLET, C. DING, H. NIEDERREITER. *Authentication Schemes from Highly Nonlinear Functions*, in "Designs, Codes and Cryptography", to appear, 2005.

[17] C. CARLET, C. DING, J. YUAN. *Linear Codes from Perfect Nonlinear Mappings and their Secret Sharing Schemes*, in "IEEE Trans. Inform. Theory", to appear, 2005.

[18] C. CARLET, P. GABORIT. *Hyper-bent functions and cyclic codes*, in "ournal of Combinatorial Theory", to appear, 2005.

[19] C. CARLET, J. YUCAS. *Piecewise Constructions of Bent and Almost Optimal Boolean Functions*, in "Designs, Codes and Cryptography", to appear, 2005.

[20] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *On cosets of weight 4 of binary BCH codes of length 2^m (m odd), with minimal distance 8, and exponential sums*, in "Problems of Information Transmission", vol. 41, n° 4, 2005, p. 331-348.

[21] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *Propagation characteristics of $x \mapsto 1/x$ and Kloosterman sums*, in "Finite Fields and Applications", to appear, 2005.

[22] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *The Coset Distribution of the Triple-Error-Correcting Binary Primitive BCH Codes*, in "IEEE Trans. Inform. Theory", to appear, 2005.

[23] P. CHARPIN, E. PASALIC. *Highly nonlinear resilient functions through disjoint codes in projective spaces*, in "Designs Codes and Cryptography", vol. 37, 2005, p. 319-346.

[24] P. CHARPIN, E. PASALIC, C. TAVERNIER. *On bent and semi-bent quadratic Boolean functions*, in "IEEE Trans. Inform. Theory", Regular paper, to appear, 2005.

[25] F. DIDIER. *A new bound on the block error probability after decoding over the erasure channel*, in "IEEE Trans. Inform. Theory", to appear, 2006.

[26] E. FILIOL. *Cryptologie malicieuse ou virologie cryptologique ?*, in "MISC - Le journal de la sécurité informatique", vol. 20, juillet 2005.

[27] E. FILIOL. *Evaluation des logiciels antiviraux : quand le marketing s'opposeà la technique*, in "MISC - Le journal de la sécurité informatique", vol. 21, septembre 2005.

[28] E. FILIOL. *La simulabilité des tests statistiques*, in "MISC - Le journal de la sécurité informatique", vol. 22, novembre 2005.

[29] E. FILIOL. *Le virus Bradley ou l'art du blindage total*, in "MISC - Le journal de la sécurité informatique", vol. 20, juillet 2005.

[30] E. FILIOL. *Le virus Ymun : la cryptanalyse sans peine*, in "MISC - Le journal de la sécurité informatique", vol. 20, juillet 2005.

[31] E. FILIOL. *Le virus* PERRUN *: méfiez vous des images... et des rumeurs*, in "MISC - Le journal de la sécurité informatique", vol. 18, mars 2005.

[32] E. FILIOL. *Le virus* WHALE *: le virus se rebiffe*, in "MISC - Le journal de la sécurité informatique", vol. 19, mai 2005.

[33] E. FILIOL. *SCOB/PADODOR : quand les codes malveillants collaborent*, in "MISC - Le journal de la sécurité informatique", vol. 17, January 2005.

[34] J. FRIEDMAN, R. MURTY, J. TILLICH. *Spectral estimates for Abelian Cayley graphs*, in "Journal of Combinatorial Theory Ser.B", in Press, 2005.

[35] J. FRIEDMAN, J. TILLICH. *Generalized Alon-Boppana Theorems and Error-Correcting Codes*, in "SIAM Journal of Discrete Mathematics", in Press, 2005.

[36] P. GABORIT, C. S. NEDELOAIA, A. WASSERMANN. *Weight enumerators of duadic and quadratic residue codes*, in "IEEE Trans. Inf. Theory", vol. 51, n^o 1, January 2005, p. 402-407.

[37] G. KABATIANSKY. *Codes for copyright protection:the case of two pirates*, in "Information Transmission Problems", vol. 41, n^o 2, 2005, p. 123-127.

[38] Y. LAIGLE-CHAPUY. *Permutation Polynomials and applications to coding theory*, in "Finite Fields and Applications", To appear, 2005.

[39] C. LAURADOUX. *Machine virtuelle et Honeypot*, in "MISC - Le journal de la sécurité informatique", version allemande dans Multi-System, Internet, Security & Cookbook, n. 1, vol. 21, Septembre 2005.

[40] C. LAURADOUX. *Timing Attack et Hyperthreading*, in "MISC - Le journal de la sécurité informatique", version allemande dans Multi-System, Internet, Security & Cookbook, n. 1, Septembre 2005, vol. 20, Juillet 2005.

[41] P. LOIDREAU. *Pour quelques bits d'information*, in "MISC - Le magazine de la sécurité informatique", n° 20, Juillet-Août 2005.

Publications in Conferences and Workshops

[42] I. ANDRIYANOVA, J.-P. TILLICH, J.-C. CARLACH. *Asymptotically Good Codes with High Iterative Decoding Performances*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", September 2005, p. 850-854.

[43] I. ANDRIYANOVA, J.-P. TILLICH, J.-C. CARLACH. *A new family of codes with high iterative decoding performances*, in "Proceedings of ICC2006, Istambul, Turquie", to appear, June 2006.

[44] F. ARNAULT, T. BERGER. *F – FCSR: Design of a new class of stream ciphers*, in "Fast Software Encryption, FSE 2005", Lecture Notes in Computer Science, n° 3557, Springer-Verlag, 2005, p. 83-97.

[45] F. ARNAULT, T. BERGER, C. LAURADOUX. *Description of F-FCSR-8 and F-FCSR-H stream ciphers*, in "SKEW - Symmetric Key Encryption Workshop", Aarhus, Danemark, An ECRYPT STVL event, May 2005.

[46] D. AUGOT, M. BARDET, J. FAUGÈRE. *Decoding cyclic codes with algebraic systems*, in "Joint BeNeLuxFra Conference in Mathematics, Gand, Belgique", May 2005.

[47] D. AUGOT, M. FINIASZ, N. SENDRIER. *A Family of Fast Syndrome Based Cryptographic Hash Function*, in "Ecrypt Conference on Hash Functions, Krakow, Poland", June 2005.

[48] D. AUGOT, M. FINIASZ, N. SENDRIER. *A Family of Fast Syndrome Based Cryptographic Hash Functions*, in "Progress in Cryptology - Mycrypt 2005", E. DAWSON, S. VAUDENAY (editors). , LNCS, n° 3715, Springer-Verlag, 2005, p. 64-83.

[49] C. BERBAIN, O. BILLET, A. CANTEAUT, N. COURTOIS, B. DEBRAIZE, H. GILBERT, L. GOUBIN, A. GOUGET, L. GRANBOULAN, C. LAURADOUX, M. MINIER, T. PORNIN, H. SIBERT. DECIM*: a new stream cipher for hardware applications*, in "Proceedings of SKEW - Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT", Soumis au projet européen eSTREAM, en réponse à Call for Stream Cipher Primitives, Network of Excellence in Cryptology ECRYPT, May 2005, http://www.ecrypt.eu.org/stream/.

[50] C. BERBAIN, O. BILLET, A. CANTEAUT, N. COURTOIS, H. GILBERT, L. GOUBIN, A. GOUGET, L. GRANBOULAN, C. LAURADOUX, M. MINIER, T. PORNIN, H. SIBERT. SOSEMANUK*: a fast oriented software-oriented stream cipher*, in "Proceedings of SKEW - Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT", Soumis au projet européen eSTREAM, en réponse à Call for Stream Cipher Primitives, Network of Excellence in Cryptology ECRYPT, May 2005, http://www.ecrypt.eu.org/stream/.

[51] T. BERGER, A. CANTEAUT, P. CHARPIN, Y. LAIGLE-CHAPUY. *On Almost Perfect Nonlinear mappings*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", to appear, September 2005.

[52] T. BERGER, M. MINIER. *Two algebraic attacks against the F-FCSRs using the IV mode*, in "Advances in Cryptology - INDOCRYPT 2005", Lecture Notes in Computer Science, nº 3797, Springer-Verlag, 2005, p. 143-154.

[53] R. BHASKAR, D. AUGOT, V. ISSARNY, D. SACCHETTI. *An Efficient Group Key Agreement Protocol for Ad hoc Networks*, in "IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing", Taormina, Italy, June 2005.

[54] L. BUDAGHYAN, C. CARLET, A. POTT. *New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", March 2005, p. 306-315.

[55] T. CAMARA, H. OLLIVIER, J. TILLICH. *Constructions of quantum LDPC codes*, in "proceedings of EQUIS2005, ERATO conference on quantum information science", September 2005, p. 65-66.

[56] A. CANTEAUT. *Fast Correlation Attacks Against Stream Ciphers and Related Open Problems*, in "Proceedings of the 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005), Awaji Island, Japon", Invited talk, IEEE Press, octobre 2005.

[57] A. CANTEAUT. *Le chiffrement à flot*, in "Ecole de Jeunes Chercheurs en Algorithmique et Calcul Formel 2005, Montpellier", avril 2005.

[58] A. CANTEAUT. *Open problems related to algebraic attacks on stream ciphers*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", invited talk, March 2005, p. 1-11.

[59] C. CARLET. *Designing bent functions and resilient functions from known ones, without extending their number of variables*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", September 2005.

[60] C. CARLET. *On bent and highly nonlinear balanced/resilient functions and their algebraic immunities*, in "actes du congrès AAECC 16", article invité, 2005.

[61] C. CARLET. *On highly nonlinear S-boxes and their inability to thwart DPA attack*, in "Advances in Cryptology - INDOCRYPT 2005", Lecture Notes in Computer Science, nº 3797, Springer-Verlag, 2005, p. 49-62.

[62] C. CARLET, P. GABORIT. *On the construction of balanced Boolean functions with a good algebraic immunity*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", September 2005.

[63] C. CARLET, S. GANGOPADHYAY, S. MAITRA. *Crosscorrelation spectra of Dillon type functions*, in "actes du congrès International Workshop on Sequence Design and its Applications in Communications - IWSDA'05", 2005.

[64] C. CARLET, S. MESNAGER. *Improving the upper bounds on the covering radii of Reed-Muller codes*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", September 2005.

[65] P. CHARPIN, T. HELLESETH, V. ZINOVIEV. *The Coset Distribution of the Triple-Error-Correcting Binary Primitive BCH Codes*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", to appear, September 2005.

[66] M. CLUZEAU. *Reconstruction d'un brasseur linéaire*, in "Ecole de Jeunes Chercheurs en Algorithmique et Calcul Formel, Montpellier, France", Avril 2005.

[67] C. FAURE, P. LOIDREAU. *A new public-key cryptosystem based on the problem of reconstruction of p-polynomials*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", March 2005, p. 275-85.

[68] E. FILIOL. *Strong Cryptography Armoured Computer Viruses Forbidding Code Analysis: the* BRADLEY *virus*, in "Proceedings of the 14th EICAR Conference", 2005, p. 201-217.

[69] E. GABIDULIN, P. LOIDREAU. *On subcodes of codes in rank metric*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", to appear, September 2005.

[70] P. GABORIT. *Shorter keys for code based cryptography*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", March 2005, p. 81-91.

[71] G. KABATIANSKY, C. TAVERNIER. *List decoding of second order Reed-Muller codes*, in "Proceedings of Eight International Simposium on Communication Theory and Applications, Ambelside, UK", July 2005.

[72] C. LAURADOUX. *Collision attacks on processors with cache and countermeasures.*, in "WeWork 2005, Western European Workshop on Research in Cryptology, Leuven, Belgium", July 2005.

[73] C. LAURADOUX. *Complexité des fonctions booléennes symétriques*, in "Ecole de Jeunes Chercheurs en Algorithmique et Calcul Formel, Montpellier, France", Avril 2005.

[74] C. LAURADOUX. *Machine Virtuelle et Pot de miel*, in "Ecole Internet Nouvelle Génération, ING 2005, Montreuil sur Mer, France", Juillet 2005.

[75] F. LEVY-DIT-VEHEL, L. PERRET. *On Wagner-Magyarik Cryptosystem*, in "Proceedings of WCC'2005, Bergen, Norway", 2005, p. 285-294.

[76] P. LOIDREAU. *A Welch-Berlekamp like algorithm for decoding Gabidulin codes*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", March 2005, p. 30-39.

[77] M. MINIER. *An Integral Cryptanalysis of a five rounds version of FOX.*, in "WeWork 2005, Western European Workshop on Research in Cryptology, Leuven, Belgium", July 2005.

[78] H. OLLIVIER, J.-P. TILLICH. *Interleaved serial concatenation of quantum convolutional codes: gate imple-*

mentation and iterative error estimation algorithm, in "actes du 26th Symposium on Information Theory in the Benelux, Bruxelles, Belgique", 2005, 149.

[79] L. PERRET. *A chosen ciphertext attack on a public key cryptosystem based on Lyndon words*, in "Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)", March 2005, p. 235-45.

[80] L. PERRET. *A Fast Cryptanalysis of the Isomorphism of Polynomials with One Secret Problem*, in "Advances in Cryptology - EUROCRYPT 2005", Lecture Notes in Computer Science, n° 3494, Springer-Verlag, 2005, p. 354-71.

[81] L. PERRET. *Algorithms for solving the isomorphism of polynomials with one secret problem*, in "Joint BeNeLuxFra Conference in Mathematics, Gand, Belgique", Joint Meeting Of The Belgian (BMS), Dutch (KWG), Luxembourg And French (SMF) Mathematical Societies, May 2005.

[82] N. SENDRIER. *Encoding information into constant weight words*, in "Proceedings 2005 IEEE International Symposium on Information Theory, Adelaide, Australie", September 2005.

[83] N. SENDRIER. *Public-key cryptology based on error-correcting codes*, in "CAEN'05", Invited talk, June 2005.

[84] V. V. SHORIN, P. LOIDREAU. *Application of Groebner bases Techniques for searching new sequences with good periodic correlation properties*, in "Proceedings of 2005 International Symposium on Information Theory, ISIT 2005", September 2005.

[85] M. VIDEAU. *Symmetric Boolean functions with high nonlinearity*, in "WeWork 2005, Western European Workshop on Research in Cryptology, Leuven, Belgium", July 2005.

Internal Reports

[86] D. AUGOT, M. FINIASZ, N. SENDRIER. *A Family of Fast Syndrome Based Cryptographic Hash Function*, Rapport de Recherche, n° 5592, INRIA, June 2005, http://www.inria.fr/rrrt/rr-5592.html.

[87] D. AUGOT, F. MORAIN, C. FONTAINE, J. LENEUTRE, S. MAAG, A. CAVALLI, F. NAIT-ABDESSELAM. *Review of vulnerabilities in mobile ad-hoc networks: trust and routing protocols views*, Technical report, ACI SERAC, 2005.

[88] T. BERGER, A. CANTEAUT, P. CHARPIN, Y. LAIGLE-CHAPUY. *Almost perfect nonlinear functions*, Technical report, n° RR-5774, Rapport de Recherche INRIA, Décembre 2005, http://www.inria.fr/rrrt/rr-5774.html.

[89] P. LOIDREAU. *An Algebraic attack against Augot-Finiasz cryptosystem*, Technical report, n° RR-5662, INRIA, 2005, http://www.inria.fr/rrrt/rr-5662.html.

[90] C. S. NEDELOAIA. *Upper bounds on the dual distances of $EBCH$ codes*, Technical report, n° RR-5477, Rapport de Recherche INRIA, Janvier 2005, http://www.inria.fr/rrrt/rr-5477.html.

Miscellaneous

[91] D. AUGOT, A. BIRYUKOV, A. BRAEKEN, C. CID, H. DOBBERTIN, H. ENGLUND, H. GILBERT,

L. GRANBOULAN, H. HANDSCHUH, M. HELL, T. JOHANSSON, A. MAXIMOV, M. PARKER, T. PORNIN, B. PRENEEL, M. ROBSHAW, M. WARD. , A. CANTEAUT (editor). *Open Research Areas in Symmetric Cryptography and Technical Trends in Lightweight Cryptography*, 2005, http://www.ecrypt.eu.org/documents/D.STVL.3-2.5.pdf, Rapport du réseau d'excellence européen ECRYPT.

[92] F. DIDIER, J. P. TILLICH. *Computing the algebraic immunity efficiently*, 2006.

[93] P. GABORIT. *Clés plus courtes pour les cryptosystèmes de chiffrement basés sur des codes*, Journées "Codage et Cryptographie", Aussois, France, Février 2005.

[94] Y. LAIGLE-CHAPUY. *Polynômes de permutation et application en théorie des codes*, Journées "Codage et Cryptographie", Aussois, France, Février 2005.

[95] M. MINIER. *LILI-128 et ses attaques*, Journées "Codage et Cryptographie", Aussois, France, Février 2005.