

Rapport de Recherche

Groupe de Recherche en Complexité et Cryptographie

24 avril 1995

Table des matières

| | | |
|----------|---|-----------|
| 1 | Composition du groupe | 1 |
| 2 | Présentation des thèmes de recherche | 2 |
| 2.1 | Théorie de la complexité: Preuves Interactives et Approximation des problèmes <i>NP</i> -complets | 3 |
| 2.2 | Théorie algorithmique des nombres et théorie des codes correcteurs d'erreurs | 3 |
| 2.3 | Cryptographie à clé publique | 5 |
| 2.4 | Cryptographie Conventionnelle | 7 |
| 2.5 | Cryptographie quantique | 9 |
| 2.6 | Perspectives | 10 |
| 3 | Missions et invitations du GRECC | 11 |
| 3.1 | Invitations | 11 |
| 4 | Diffusion de la Recherche | 12 |
| 5 | Évaluation de la Recherche | 13 |
| 6 | Activités d'enseignement | 13 |

1 Composition du groupe

- Responsable: Jacques Stern (Professeur à l'École Normale Supérieure).
- Membres
 - Claude Crépeau, Chargé de Recherche au CNRS, partant en septembre 95
 - Philippe Hoogvorst, Chargé de Recherche au CNRS, arrivé en septembre 93
 - Antoine Joux, Ingénieur de l'armement, parti en septembre 93 (thèse soutenue en mai 1993)
 - Jean Marc Couveignes, Ingénieur de l'armement, thèse soutenue en juillet 94

- Serge Vaudenay, Assistant moniteur normalien à l'École Normale Supérieure, thèse prévue en mai 1995
- Louis Granboulan, Thésard, élève à l'École Normale Supérieure, au service national en 1994-95
- Ludovic Caudal, Thésard, élève à l'École Normale Supérieure de Cachan, partant en 1995
- Florent Chabaud, Thésard, Ingénieur de l'armement
- David Pointcheval, Thésard, élève à l'École Normale Supérieure, au service national en 1994-95
- Philippe Béguin, Thésard, élève à l'École Normale Supérieure
- Jean-Bernard Fischer, Thésard CIFRE (en collaboration avec THOMSON TCE)

2 Présentation des thèmes de recherche

Créé en 1988, le Groupe de Recherche en Complexité et Cryptographie (GRECC) a pour objet de contribuer au développement en France de ces deux thèmes d'étude qui se trouvent à l'interface des mathématiques et de l'informatique. Abrisé depuis l'origine par le département de mathématiques et informatique de l'École Normale Supérieure (DMI), il a été formellement intégré au LIENS en janvier 1992. Le recrutement d'un CR1 (Claude Crépeau) et le détachement comme DR du responsable du GRECC, en attendant sa nomination sur un poste ENS, ont été perçus par le Laboratoire comme le soutien des instances du CNRS au développement de ce groupe. La pérennité du GRECC paraît maintenant établie mais le départ prochain de Claude Crépeau pose un problème d'encadrement que ne résout pas l'arrivée de Philippe Hoogvorst en provenance d'un autre thème du LIENS, puisque ce dernier effectue une conversion thématique. Le groupe espère donc vivement pouvoir bénéficier dans les années qui viennent d'un recrutement au titre du CNRS.

Le groupe essaie de développer tout à la fois les aspects théoriques et pratiques de la Complexité algorithmique, ce qui l'amène à couvrir un domaine d'étude très «vertical» puisqu'il va de la théorie abstraite de la complexité et de la théorie algorithmique des nombres, à l'implantation d'algorithmes cryptographiques sur ordinateur ou sur carte à mémoire. Ce domaine d'étude se trouve assez bien décrit par la liste des grands congrès internationaux auxquels les membres du groupe participent en priorité

- FOCS (Foundations of Computer Science)
- STOC (Symposium on the Theory of Computing)
- ANTS (Algorithmic Number Theory Symposium)
- CRYPTO
- EUROCRYPT
- ACMCCS (ACM Conference on Computer and Communications Security)

2.1 Théorie de la complexité : Preuves Interactives et Approximation des problèmes \mathcal{NP} -complets

Depuis une quinzaine d'années, les progrès de la théorie des algorithmes ont permis de mettre en évidence la possibilité d'établir ou de transmettre certains faits mathématiques, non pas à l'aide d'une preuve au sens logique du terme, mais à travers un processus interactif de questions réponses aléatoires. Ces travaux ont entre autres choses conduit à la formulation de la notion de preuve «zero-knowledge».

Ces découvertes sont riches d'applications : on a ainsi pu réaliser effectivement des systèmes cryptographiques présentant des fonctionnalités entièrement nouvelles :

- systèmes à clefs publiques (où la clef de codage est publique)
- systèmes «zero-knowledge», qui autorisent l'authentification sur un canal non sécurisé et pour des architectures décentralisées.

En 1992, on a assisté à un spectaculaire «retour» des études de cryptographie puisque des concepts issus de cette discipline appliquée (celui d'interaction en particulier) ont permis de faire des progrès spectaculaires sur la question de l'approximation des problèmes \mathcal{NP} -complets. Le GRECC a participé à ce mouvement d'idées (Voir entre autre [BCY91] et [Ste93a, ABSS93]).

Citons en particulier

- La définition du «zero-knowledge» dans un modèle restreint : le modèle original suppose que l'un des participants a une puissance de calcul infinie ([BCLL91]).
- Les résultats sur l'impossibilité de définir des algorithmes d'approximation pour certains problèmes d'optimisation concernant les codes correcteurs d'erreur ou les réseaux à coordonnées entières ([Ste93a, ABSS93]). La version définitive de ce dernier travail va paraître prochainement dans un numéro spécial du JCSS, consacré aux preuves interactives et à l'approximation.

2.2 Théorie algorithmique des nombres et théorie des codes correcteurs d'erreurs

Factorisation des nombres entiers Outre la théorie de la complexité algorithmique, la cryptographie s'appuie sur la théorie des nombres, en particulier sur les questions liées à la factorisation des nombres entiers. Le groupe suit de très près les développements dans ce domaine qui conditionnent la sécurité de nombreux algorithmes cryptographiques. Il a participé, en collaboration avec des chercheurs étrangers, à l'élaboration de diverses techniques de pointe, en particulier à l'accélération du crible algébrique (Number Field Sieve), méthode de factorisation des entiers naturels proposée par Lenstra et Pollard en 1990. Cette méthode, conçue au départ pour factoriser des nombres *spéciaux* de la forme $a^b \pm c$, c petit, est heuristiquement la plus rapide de toutes les méthodes connues. Cependant, pour des entiers *généraux*, elle se heurte à des difficultés pratiques telles que la manipulation de nombres entiers gigantesques (plusieurs millions de décimales). Un des chercheurs du groupe

([Cou93]) a développé des techniques modulaires qui permettent d'éviter ces manipulations trop coûteuses et qui de plus, facilitent la parallélisation. La dernière implémentation de l'algorithme NFS faite par Arjen Lenstra, a utilisé ces améliorations et a conduit au dernier record du monde dans ce domaine.

Algorithmique sur les réseaux à coordonnées entières Un réseau est un \mathbf{Z} -module discret de \mathbf{R}^n . Réduire un réseau, c'est trouver une bonne base du réseau, formée de vecteurs assez courts et assez orthogonaux. C'est un problème largement étudié mais les solutions classiques - sauf en petite dimension- ne sont jamais constructives. Lenstra, Lenstra, Lovász, en 1983, ont obtenu un algorithme polynomial, appelé LLL, qui trouve une assez bonne base du réseau. En particulier, le premier vecteur de cette base est suffisamment court pour jouer le même rôle que le plus court vecteur du réseau.

L'algorithme LLL, qui utilise l'arithmétique rationnelle pour manipuler de très grands nombres est extrêmement inefficace. Les implantations pratiques qui tournent (par exemple aux Bell Labs, à l'Université de Francfort et au LIENS) substituent à l'arithmétique rationnelle l'arithmétique flottante de la machine. L'analyse théorique qui justifie et contrôle cette substitution est très délicate et a été principalement menée par C. Schnorr. Le GRECC s'est attaché à concevoir un algorithme parallèle de réduction de réseau qui intègre les méthodes numériques de Schorr. Une solution élégante a ainsi pu être proposée ([Jou93b, Jou93a]), qui est l'un des résultats d'une thèse soutenue récemment.

Calculs explicites d'objets mathématiques complexes Le groupe a également utilisé l'algorithme LLL, décrit ci-dessus, pour calculer explicitement des objets mathématiques complexes : les revêtements de la sphère ramifiés au dessus de trois points seulement, appelés aussi *Dessins d'Enfants*. L'étude de ces objets remonte au siècle dernier mais ils ont été remis au goût du jour par «l'esquisse d'un programme» rédigée il y a quelques années par Alexandre Grothendieck. Au cours de ce travail, ont été obtenus des résultats sur les propriétés de rationalité de ces revêtements ([Cou94d, Cou94c]).

A partir des dessins, il est possible de construire explicitement des objets mathématiques ayant certaines propriétés particulièrement intéressantes. Par exemple on peut ainsi tenter de résoudre certaines instances du problème de Galois inverse. C'est ainsi que le GRECC a pu réaliser la construction et le calcul explicite d'un dessin correspondant à une extension régulière de $Q(T)$ de groupe de Galois M_{24} ([Gra94]). On connaissait l'existence d'une telle extension sans en avoir la description. Cela prouve l'intérêt des techniques de calcul de dessins développées par le groupe dans [Cou94a] et [CG94a] qui ont permis de construire explicitement des objets mathématiques impossibles à traiter par les méthodes usuelles du calcul formel.

Calculs du nombre de points d'une courbe elliptique C'est René Schoof qui a proposé en 1985 le premier algorithme polynomial pour le calcul du nombre de points rationnels sur une courbe elliptique définie sur un corps fini. Malheureusement sa méthode restait impraticable et ce sont des idées d'Elkies et d'Atkin qui ont permis d'aboutir à des calculs explicites au moins dans le cas où le corps est primitif (F_p) ou du moins de caractéristique

assez grande. L'application de ces méthodes au calcul de la cardinalité d'une courbe elliptique sur un corps de type F_{2^k} est restée un problème ouvert pendant quelques années. Or le cas de la caractéristique 2 est le plus utile dans les applications pratiques (cryptographie en particulier).

Ce problème a été résolu au sein du GRECC en utilisant la géométrie des groupes formels attachés aux courbes elliptiques. Une implémentation réalisée en collaboration avec le laboratoire de l'École Polytechnique a démontré l'efficacité de cette méthode.

Théorie des codes À plusieurs reprises, un lien s'est établi entre les recherches du GRECC et la théorie des codes. C'est ainsi que les chercheurs du GRECC ont été amenés à étudier divers problèmes de codes.

- Génération de familles codes linéaires dit intersectants [CS91a] [CS91b].
- Familles de codes correcteurs d'erreurs constructibles en temps polynomial, en particulier, codes dont les vecteurs non nuls ont tous presque le même poids ([LS91, LS92a]).

De façon inattendue, la seconde famille fournit les meilleures bornes asymptotiques pour les solutions effectives du «kissing number problem» (Placer autant de boules de rayon un que possible au contact d'une boule donnée). ([LS92b, LS94]). Dans le même ordre d'idées, la dérandomisation des algorithmes probabilistes, étudiée en particulier par Alon et al. et Naor et Naor, peut se ramener à des problèmes de théorie des codes. L'utilisation de méthodes de construction de codes algébriques telles que celles de [LS92a] pourrait donc permettre d'améliorer certains résultats.

Enfin, les codes interviennent à plusieurs reprises dans la construction de protocoles basés sur les phénomènes quantiques [BBCS92, BCJL93, CS95, CT95]. On y reviendra plus loin.

2.3 Cryptographie à clé publique

L'irruption de méthodes mathématiques sophistiquées en cryptographie remonte à l'introduction de la cryptographie à clé publique par Diffie et Hellman en 1976. Cette méthode, reposant sur une dissymétrie entre la clé de chiffrement supposée disponible pour tous et la clé de déchiffrement, réservée à l'utilisateur légitime, est encore aujourd'hui illustrée par un très petit nombre d'exemples, le principal étant le système RSA, du nom de ses auteurs Rivest, Shamir et Adleman.

Cela dit, et contrairement à une opinion répandue, la cryptographie à clé publique ne sert pas seulement, et sans doute même pas principalement, à chiffrer. Elle autorise diverses autres fonctionnalités riches d'applications

- la **signature**, où chaque utilisateur peut attacher à un message m une valeur qui dépend d'une clé secrète et dont la validité peut être vérifiée par toute personne en possession de la clé publique correspondante, ce qui la rend opposable aux tiers, comme une signature manuscrite conventionnelle. Le système RSA permet de signer, mais d'autres systèmes ont également été proposés comme le DSS (Digital Signature System), basé sur le problème du logarithme discret.

- l’identification, où un utilisateur prouve son identité à un tiers lors d’une communication ou une transaction (login, contrôle d’accès, etc.).

Signature Comme on vient de le dire, les deux principaux schémas de signature à clé publique sont le RSA et le DSS. Pour ces deux schémas, le signeur doit effectuer une exponentiation modulaire. Or, en pratique, ces signatures sont souvent effectuées par des cartes à puces qui ont une puissance de calcul très limitée qui ne leur permet pas de réaliser en un temps raisonnable ces exponentiations. Une alternative à ce problème est d’utiliser la puissance de calcul d’un serveur (terminal bancaire, téléphonique, etc) en lui déléguant des calculs. Cette idée a été introduite en 1988 par Matsumoto, Kato et Imai. Mais aucun des protocoles existant n’étaient sécurisés. En collaboration avec Jean-Jacques Quisquater (Université Catholique de Louvain, Belgique), nous avons pu proposer des méthodes d’accélération plus sûres, tant pour le RSA ([BQ94a, BQ95]) que pour le DSS ([BQ94b]).

Procédés d’identification Au plan pratique, Fiat et Shamir ont donné en 1986 une application de la notion de protocole zero-knowledge en imaginant un procédé d’identification fondé sur l’utilisation d’une clé secrète mais ne révélant aucune information (en particulier pas la clé, au contraire des méthodes du type mot-de-passe). Le GRECC a examiné la possibilité d’arriver à un résultat analogue en n’autorisant que des calculs très simples. Dans cet ordre d’idées, l’équipe a récemment mis au point toute une série de protocoles d’identification simples :

- l’un fondé sur la mise en œuvre de codes correcteurs d’erreurs ([Ste93b]).
- un autre reposant sur le problème du 3-couplage [LC94]. Il reste des problèmes combinatoires à résoudre pour compléter l’étude de ce schéma.
- un autre encore basé sur un nouveau problème \mathcal{NP} -complet, inspiré de la théorie des réseaux de neurones ([Poi95]).
- un autre enfin utilisant un problème original d’équations linéaires contraintes ([Ste94]). Ce dernier protocole a l’avantage de n’utiliser que des clés de taille comparable à celles de la cryptographie conventionnelle (64 à 80 bits), ce qui apporte une réponse à un problème posé depuis longtemps en cryptographie à clé publique.

Analyse cryptographique L’analyse cryptographique est la partie de la cryptographie qui s’efforce de recouvrer la partie secrète d’un message, d’un code ou d’un outil cryptographique, à partir des éléments publics. Une méthode très efficace en ce domaine est la recherche de relations de dépendance linéaires à coefficients modérés en utilisant l’algorithme de Lenstra, Lenstra et Lovàsz (LLL), mentionné plus haut. Comme on l’a mentionné plus haut, le GRECC s’est doté d’une implantation performante de LLL qui lui permet d’expérimenter les algorithmes, issus d’une analyse théorique et de les valider. La liste des «cryptanalyses» les plus récentes à l’actif du groupe est la suivante :

- Cassage d’un cryptosystème à clef publique présenté à Eurocrypt’90 basé sur l’utilisation de knapsacks modulaires ([JS91a, CJS91]).

- Amélioration des attaques contre les knapsacks entiers, travail réalisé en compétition ([JS91b]), puis en collaboration ([CJL⁺93]) avec les équipes de Schnorr (Francfort) et Odlyzko (Bell Labs).
- Attaque contre des systèmes cryptographiques fondés sur la factorisation des groupes ([SBM93]).
- Attaque contre une fonction de hachage cryptographique proposée par Damgård ([JG94, JS94]). La fonction de Damgård a été attaquée à plusieurs reprises mais nous sommes les premiers à avoir proposé une méthode autorisant des calculs explicites.

En dehors des méthodes utilisant l'algorithme LLL, nous nous sommes intéressés à l'analyse de la sécurité des systèmes basés sur la difficulté du décodage général des codes linéaires (système de Mc Eliece et, plus récemment procédé d'identification de Stern, mentionné plus haut). En utilisant des algorithmes existants et en les optimisant, il a été possible d'améliorer les performances des attaques contre le cryptosystème de McEliece. Il ne s'agit pas à proprement parler de cryptanalyse puisque le système n'est pas cassé mais les paramètres minimaux assurant la sécurité sont ainsi plus finement évalués. Un travail analogue pour le procédé de Stern a aussi été mené dans [Cha94]. De nouveaux développements ont été soumis à Eurocrypt'95 [CC].

Nous avons également, dans un travail mené avec Don Coppersmith (IBM Yorktown), montré qu'un procédé de signature introduit par Adi Shamir et basé sur les permutations birationnelles, pouvait être attaqué avec succès ([CSV94]). Notre cryptanalyse utilise des méthodes empruntées à la théorie de Galois et, là encore, permet des calculs explicites. Adi Shamir a cité notre travail comme le meilleur publié en cryptographie durant l'année 1993. Nous lui laissons bien entendu la responsabilité de cette assertion mais notons avec plaisir qu'elle montre la notoriété internationale que le GRECC a acquise en peu d'années dans le domaine de la cryptologie.

2.4 Cryptographie Conventiionnelle

De façon surprenante, le développement de la cryptographie à clé publique a amené, par ricochet, des progrès sur les méthodes conventionnelles. Il faut noter en effet que la cryptographie à clé publique n'élimine pas le recours aux procédés conventionnels, pour au moins deux raisons :

- les méthodes de cryptographie à clé publique restant relativement lentes, elles ne sont essentiellement utilisées (à part pour signer), que pour des échanges de clés secrètes conventionnelles.
- Certains problèmes que rencontre la cryptographie ne sont pratiquement résolus que par des voies traditionnelles : c'est le cas pour la définition de fonctions de condensation (ou de hachage) associant à un (long) message un condensé de quelques centaines de bit.

S'agissant précisément des fonctions de chiffrement symétriques (comme le DES, Data Encryption Standard) ou des fonctions de hachage, deux méthodes très générales d'évaluation et d'attaque sont apparues récemment :

- la cryptanalyse différentielle., due à Biham et Shamir, et basée sur l'étude statistique de la répartition des différences (xors) entre clairs et chiffrés
- La cryptanalyse linéaire introduite par Matsui au congrès Eurocrypt'93 et basée sur la recherche de relations linéaires entre bits de clair, de chiffré et de clé, ayant un biais significatif

Ces deux cryptanalyses appliquées à DES sont les premières à être plus rapides que la recherche exhaustive. Le GRECC participe au renouveau de la recherche sur la cryptologie conventionnelle et une thèse sur le sujet sera soutenue en 1995.

Fonctions de Hachage On vient de mentionner le concept de fonction de hachage. On requiert en général que l'opération se fasse de façon qu'il soit virtuellement impossible de calculer deux messages ayant même condensé (on parle de collision). Le GRECC a ainsi étudié la fonction de hachage FFT-Hash 2 proposée par Claus Schnorr au colloque Eurocrypt'92 pour laquelle il a trouvé des collisions ([Vau93a]). Le groupe a également fait une étude assez générale des fonctions de hachage et les a utilisées dans la mise au point d'un système cryptographique permettant l'authentification sans recours au zero-knowledge ([Vau93b]).

Plus récemment, le GRECC a également mis en évidence certaines faiblesses de la fonction de hachage MD4 proposée par R. Rivest en obtenant des collisions pour une version simplifiée ([Vau95]).

Chiffrement symétrique On a parlé plus haut des deux méthodes générales de cryptanalyse (différentielle et linéaire). En utilisant une approche basée sur l'utilisation systématique de la transformée de Fourier des fonctions booléennes, le groupe a pu mettre en évidence des propriétés de dualité de ces deux cryptanalyses, et donc leur complémentarité [CV94].

Le GRECC a aussi porté son attention sur la fonction de chiffrement SAFER proposée par J. Massey et dédié aux microprocesseurs 32 bits. Il a en particulier proposé une attaque sur une variante de SAFER ([Vau95])

Approche théorique de la cryptographie conventionnelle S'inspirant des cryptanalyses dont on vient de parler dans les deux paragraphes précédents, le GRECC a entrepris d'élaborer une théorie générale des fonctions cryptographiques conventionnelles (hachage et chiffrement). Cette théorie s'est pour l'instant développée suivant deux axes

- **La notion de multipermutation** Les fonctions cryptographiques primitives utilisent des boîtes pour *diffuser* l'information. La sécurité est liée à la complexité de l'interconnexion de ces boîtes. Afin de rendre la fonction sûre, les boîtes doivent réaliser une diffusion parfaite: toute perturbation de peu d'entrées doit entraîner la perturbation de beaucoup de sorties [Vau95]. Cela a été formalisé par la notion originale de *multipermutation*. Cet objet combinatoire, apparu pour la première fois dans [SV94a], est relié

aux carrés latins, aux codes MDS, aux matrices orthogonales et aux plans projectifs finis.

- **Le concept d’attaque générique** Les outils universels, pour l’attaque des primitives cryptographiques, sont la recherche exhaustive et l’utilisation du paradoxe des anniversaires. Leur généralisation systématique formalise des classes d’attaques génériques, en utilisant des notions inspirées de la théorie des bases de données relationnelles et de la sémantique. L’étude de la sécurité des primitives face à ces classes d’attaques peut être envisagée en utilisant certains domaines de la théorie des graphes : les graphes d’expansion, les graphes de Cayley et les flots.

Protocoles cryptographiques Les protocoles cryptographiques sont des algorithmes à plusieurs participants où certaines informations secrètes sont traitées. On considère, par exemple, le problème général du calcul partagé d’une fonction : deux participants A et B veulent calculer une fonction $f(x, y)$ sur données a et b , a étant connue de A et b connue de B , sans se révéler mutuellement a et b , mais seulement le résultat $f(a, b)$. On considère également le scénario où une information secrète doit être partagée entre n participants de façon que k d’entre eux doivent contribuer leur part pour que le secret soit découvert : c’est le problème du «partage du secret». Sans en faire l’axe principal de ses recherches, le GRECC ne néglige pas l’étude des protocoles.

C’est ainsi que, récemment, le groupe a envisagé les possibilités cryptographiques d’un individu isolé équipé d’un paquet de cartes à jouer [CK93]. La problématique était d’établir ce qui peut être calculé secrètement par rapport à soi-même. Ce point de vue pourrait ouvrir de nouvelles perspectives.

En matière de partage du secret, un problème important est d’optimiser la taille des parts : en effet, un fait bien connu dans la théorie des partages de secrets parfaits (au sens de la théorie de l’information) est que la taille des parts détenues par chaque personne doit être supérieure ou égale à celle du secret. Si l’on requiert une sécurité basée seulement sur la complexité algorithmique, on peut s’affranchir de cette contrainte comme l’a montré H. Krawczyk à Crypto’93 pour les structures d’accès seuil. En collaboration avec Antonella Cresti (Université de Rome, Italie), nous avons pu généraliser ce résultat à toutes les structures d’accès ([BC95])

2.5 Cryptographie quantique

A la suite des travaux de G. Brassard et C. Bennett, il a été proposé d’utiliser des phénomènes quantiques dans la construction de protocoles cryptographiques. Depuis quelques années, il existe aux États-Unis un prototype de transmetteur quantique démontrant le potentiel de ces idées. Le GRECC participe à l’élaboration de la cryptographie quantique : il a ainsi montré comment on peut utiliser la polarisation des photons pour construire des primitives cryptographiques (voir [BC91] [Cré93] [BBCS92]). Sont également liés à la cryptographie quantique certains travaux ayant pour but de démontrer la sécurité des solutions proposées précédemment [BBCM95] [BCJL93]. Le GRECC a enfin participé à des recherches de physique fondamentale sur la téléportation d’un état quantique [BBC⁺93].

Dernièrement, nous avons surtout concentré nos recherches sur l'élaboration de protocoles efficaces pour des tâches cryptographiques. Une fois encore, ces protocoles nécessitent l'utilisation de la théorie des codes. C'est ainsi que nous avons mis au point avec Louis Salvail (Université de Montréal) un protocole d'identification quantique permettant à deux personnes de vérifier qu'ils possèdent un mot de passe commun sans se le révéler. ([CS95]). Il faut noter que la cryptographie quantique ouvre des perspectives de coopération avec les physiciens de l'École Normale Supérieure. Un autre sujet, le *calcul quantique* éveille également l'intérêt de nos collègues physiciens. Il s'agit d'une approche nouvelle de théorie de la complexité qui envisage la mise en œuvre de machines dont l'évolution réalise des superpositions d'états quantiques. Les premiers résultats obtenus dans ce domaine sont impressionnants puisque ces machines (si elles voyaient le jour) seraient à même de réaliser des tâches au delà des limites des calculateurs actuels. Sans participer forcément à ces recherches malgré tout quelque peu spéculatives, le GRECC compte suivre de près l'évolution du domaine.

2.6 Perspectives

Un certain nombre d'éléments prospectifs ont été déjà évoqués ci-dessus, comme par exemple la question du calcul quantique pour lequel nous avons prévu la visite à l'ENS d'Andy Yao (Princeton University), pour juin 96.

Nous comptons également ouvrir de nouvelles perspectives de recherche selon les axes suivants :

Génération déterministe d'aléas Le GRECC a déjà fourni un travail considérable dans l'étude de ce sujet difficile et qui a donné lieu récemment à des résultats profonds liant les fonctions à sens uniques de la cryptographie et les générateurs de pseudo-aléa. Ce travail préliminaire devrait être parachevé prochainement grâce à la visite en juin 95 de Mike Luby (ICSI, Berkeley), expert reconnu du domaine. Nous devrions être alors prêts à obtenir nos propres résultats et comptons nous concentrer sur deux questions

- la mise en évidence de nouveaux «bits difficiles» : il résulte en effet de résultats de Yao d'une part, Goldreich et Levin d'autre part, que tout «bit difficile» donne lieu à un générateur de pseudo-aléa. Une série de travaux de Shamir, Schnorr, Micali, Blum et autres a montré que les bits de poids fort de RSA ou du logarithme discret sont difficiles. Le résultat s'étend aux bits de poids faible mais la question des bits centraux est un problème ouvert réputé difficile. Nous pensons avoir quelques idées au moins pour le cas du logarithme discret.
- la question du rendement : chaque bit d'aléa produit par un générateur fonctionnant sur la base d'un bit difficile a un coût en terme de complexité algorithmique. Ce coût est mesuré en fonction d'un paramètre de sécurité qui mesure la taille des nombres manipulés. En substituant à la théorie des nombres la théorie des codes, comme nous l'avons fait pour l'identification, nous avons l'espoir de produire un aléa avec un rendement linéaire.

Les travaux évoqués ci-dessus sont naturellement susceptibles d'applications pratiques.

Amélioration des procédés de signature Comme on l'a mentionné plus haut, les procédés de signature en usage ne sont pas totalement satisfaisants pour diverses raisons

1. ils nécessitent le calcul d'exponentielles modulaires, ce qui excède les possibilités des cartes à microprocesseur bas-coût
2. ils ont une taille relativement élevée (512 bits pour RSA, 320 bits pour DSS), ce qui interdit par exemple la signature individuelle de messages de petite taille (comme les paquets des transmissions par paquets)

Il y a là, à l'évidence, des enjeux théoriques et économiques importants. Notre projet est d'entreprendre des recherches sur les deux questions. S'agissant de l'amélioration des performances, nous sommes convaincus qu'un compromis temps/mémoire est possible. Pour ce qui est des signatures de taille réduite, la seule proposition jamais faite (par Matsumoto et Imai) vient d'être cassée. Nous croyons être en mesure de simplifier la méthode d'attaque et, éventuellement, de pouvoir ainsi réparer le procédé de signature, en contrant l'attaque.

Recherche de nouveaux systèmes cryptographiques Il s'agit là d'une question sur laquelle il faut avancer avec prudence puisque les meilleurs experts ont vu parfois leur propositions mises en échec. Nous pensons néanmoins pouvoir progresser sur un scénario qui n'a pas encore reçu toute l'attention souhaitable et que nous appelons échange de clés dissymétrique. Il s'agit d'autoriser un échange de clés entre deux entités cryptographiques : un serveur doté d'une puissance de calcul importante et un client aux capacités réduites (par exemple une carte à microprocesseur). Un tel système pourrait avoir des applications sur les problèmes de contrôle d'accès. Nous pensons aborder là encore le problème sous l'angle de la théorie des codes.

Généralisation de la cryptanalyse linéaire/différentielle Forts de notre succès sur la mise en évidence d'une dualité entre les deux méthodes de cryptanalyse, nous espérons pouvoir unifier voire améliorer les deux techniques en nous plaçant dans le cadre des tests statistiques généraux. Il nous semble en effet que les progrès récents n'ont pas épuisé le potentiel des méthodes proposées. Par ailleurs, l'expérience acquise devrait nous permettre, le moment venu, de proposer, le cas échéant, de nouveaux systèmes conventionnels (hachage ou chiffrement).

3 Missions et invitations du GRECC

3.1 Invitations

Professeurs et directeurs de recherche invités

- Adi Shamir (Weitzmann Institute),
février 1992 – juillet 1992.
- Claus Schnorr (Université de Francfort),
avril 1993.

- László Babai (Université de Chicago), mars 1994.
- Gilles Brassard (Université de Montréal), septembre 1994 – janvier 1995.
- Michael Luby (International Computer Science Institute and UC Berkeley), juin 1995.

Post-doc invités

- Olivier Delos (Université de Louvain), mars 1994.
- Antonnella Cresti (Université de Rome), mars 1994 – juillet 1994.
- Alain Tapp (Université de Montréal), mai 1994 – juillet 1994.
- Marc Joye (Université de Louvain), novembre et décembre 1994.
- Lars Knudsen, février 1995 – février 1996.

4 Diffusion de la Recherche

- Organisation à l'École Normale Supérieure, d'un séminaire régulier. Parmi les conférenciers récents: M. Luby (International Computer Science Institute and UC Berkeley), U. Maurer (ETH, Zurich – Suisse), P. Hajnal (Szeged – Hongrie), G. Brassard (Montréal – Canada), Y.Desmedt (Milwaukee – USA), M. Karpinski (Bonn – Allemagne), A. Haken (Champaign – Illinois – USA), J. Patarin (Bull CP8), F. Arnault (Limoges – France).
- Organisation, en Septembre 1991 au CIRM de Luminy, d'une conférence internationale sur la cryptographie. (parmi les participants: Shamir, Yao, Micali, Goldwasser, Goldreich, Levin, Chaum, Schnorr, ...).
- Organisation, en Octobre 1993 à Cargèse d'une réunion des participants à l'appel d'offre des PRC Codage, complexité, compression et cryptographie.
- Organisation, en Mars 1995 à l'École Normale Supérieure, Paris, d'une réunion des participants à l'appel d'offre des PRC Codage, complexité, compression et cryptographie,
- Organisation, en Septembre 1995 au CIRM de Luminy, d'une conférence internationale sur la cryptographie.

5 Évaluation de la Recherche

- J. Stern :
 - membre du comité de programme d'Eurocrypt'91, Eurocrypt'92, Eurocrypt'94 et Eurocrypt'95,
 - membre du comité de programme d'Eurocode 92,
 - membre du Comité de programme, ACM Conference on Security and privacy 1993 et 1994; président du comité en 1996,
 - membre du Comité de programme, STACS 95.
- C. Crépeau :
 - Éditeur Associé à la Complexité et la Cryptographie de l'«IEEE Transactions on Information Theory» (1/95 – 1/98)
 - membre du comité de rédaction du «Journal of Cryptology» (1/91-1/95)
 - membre du comité de programme d'«Eurocrypt'94» et de «XIV International Conference of the Chilean Computer Science Society»

6 Activités d'enseignement

- 2^e cycle :
 - MMFAI: J. Stern, A. Joux, S. Vaudenay.
 - X-tronc commun (vacations): S. Vaudenay.
 - Asian Institute of Technology, Chiang-Mai, Thaïlande: J. Stern, C. Crépeau.
 - Maîtrise d'Informatique Orsay: C. Crépeau.
 - Université de Montréal: C. Crépeau.
 - ENSTA 2^{ème} année: F. Chabaud.
 - ENSTA 3^{ème} année: C. Crépeau, A. Joux.
 - IMAC 3^{ème} année: D. Pointcheval, S. Vaudenay.
- 3^e cycle :
 - filière Algorithmique, Complexité et Cryptographie du du DEA d'Informatique mathématique (IMA): J. Stern, C. Crépeau.
 - Université de Montréal: C. Crépeau.

Références

- [ABSS93] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximating problems defined by linear constraints. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 586–597, 1993. à paraître dans JCSS.
- [BBC⁺93] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state by dual classical and EPR channels. *Physical Review Letter*, 70:1895–1898, 1993.
- [BBCM94] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification (abstract). In *Proceedings of the IEEE Symposium on Information Theory*, page 350, 1994.
- [BBCM95] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 1995. à paraître.
- [BBCS92] C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer protocols. In *Advances in Cryptology: Proceedings of CRYPTO'91*, volume 576 of *LNCS*, pages 351–366. Springer-Verlag, 1992.
- [BC91] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology: Proceedings of CRYPTO'90*, volume 537 of *LNCS*, pages 49–61. Springer-Verlag, 1991.
- [BC95] P. Béguin and A. Cresti. General short non perfect secret sharing schemes. In *Advances in Cryptology: Proceedings of Eurocrypt'95*, *LNCS*. Springer-Verlag, 1995. to appear.
- [BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *29th Symposium on Foundations of Computer Science*, pages 42–52. IEEE, 1993.
- [BCLL91] G. Brassard, C. Crépeau, S. Laplante, and C. Léger. Computationally convincing proofs of knowledge. In *Proceedings of STACS'91*, volume 480 of *LNCS*, pages 251–262. Springer-Verlag, 1991.
- [BCY91] G. Brassard, C. Crépeau, and M. Yung. Constant-round perfect zero-knowledge computationally convincing protocols. *Theoretical Computer Science*, 84:23–52, 1991.
- [BN94] P. Béguin and D. Naccache. Breacking an improved version of a "more flexible exponentiation with precomputation". Presented at the rump session of CRYPTO '94, 1994.
- [BQ93a] P. Béguin and J.-J. Quisquater. Accélération de calculs cryptographiques à l'aide d'un serveur non sécurisé. In *Journées de Cargèse: Complexité, Codage, Compression et Cryptographie*, pages 13 – 25, 1993.

- [BQ93b] P. Béguin and J.-J. Quisquater. Efficient inverse cubic RSA computations aided by a powerful untrusted server. Presented at the rump session of CRYPTO'93, 1993.
- [BQ94a] P. Béguin and J.-J. Quisquater. Resistant server-aided secret computations for public-key cryptosystems. In B. Macq, editor, *Proceedings of the Fifteenth Symposium on Information Theory in the Benelux*, pages 127–131. 'Werkge-meenschap voor Informatie- en Communicatie theorie', The Netherlands, 1994.
- [BQ94b] P. Béguin and J.-J. Quisquater. Secure acceleration of DSS signatures using insecure server. In *Advances in Cryptology Asiacrypt '94*, LNCS. Springer-Verlag, 1994. To appear.
- [BQ95] P. Béguin and J.-J. Quisquater. Acceleration of RSA signatures using an insecure server. Submitted to Crypto '95, 1995.
- [CC] A. Canteaut and F. Chabaud. A general improvement of the previous attacks on McEliece's cryptosystem. Non publié.
- [CDFdRS94] J.-M. Couveignes, J. F. Diaz-Frias, M. de Rougemont, and M. Santha. On the interactive complexity of graph reliability. In *14th FSTTCS Foundations of Software Technology and Theoretical Computer Science*. Springer, 1994.
- [CG94a] J.-M. Couveignes and L. Granboulan. Dessins from a geometric point of view. In *Grothendieck's dessins d'enfants*, Lecture Notes in Math. Cambridge University Press, 1994. Disponible comme LIENS-94-2.
- [CG94b] J.-M. Couveignes and L. Granboulan. Explicit computation of some M24 covering. En préparation, 1994.
- [Cha93] F. Chabaud. Asymptotic analysis of probabilistic algorithms for finding short codewords. In P. Camion, P. Charpin, and S. Harari, editors, *EUROCODE'92*, volume 339 of *CISM Courses and Lectures*, pages 175–183. Springer-Verlag, 1993.
- [Cha94] F. Chabaud. On the security of some cryptosystems based on error-correcting codes. In *Advances in Cryptology: Proceedings of EUROCRYPT'94*, LNCS. Springer-Verlag, 1994. To appear.
- [CJL⁺93] M. J. Coster, A. Joux, B. A. LaMacchia, A. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2:11–128, 1993.
- [CJM94] J.-M. Couveignes, A. Joux, and F. Morain. évaluation des sommes de caractères liées aux courbes elliptiques à multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire de nombre de classes 2. En préparation, 1994.

- [CJS91] Y. M. Chee, A. Joux, and J. Stern. The cryptanalysis of a new public-key cryptosystem based on modular knapsacks. In J. Feigenbaum, editor, *Advances in Cryptology: Proceedings of CRYPTO'91*, volume 576 of *LNCS*, pages 204–212. Springer-Verlag, 1991.
- [CK93] C. Crépeau and J. Kilian. Discreet solitary games. In *Advances in Cryptology: Proceedings of CRYPTO'93*, volume 537 of *LNCS*, pages 319–330. Springer-Verlag, 1993.
- [CM94] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In *First Algorithmic Number Theory Conference*, Lecture Notes in Math., 1994.
- [Cou93] J.-M. Couveignes. Computing a square root for the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Math.*, pages 95–102. Springer-Verlag, 1993.
- [Cou94a] J.-M. Couveignes. Calcul et rationalité de fonctions de Belyi en genre 0. *Annales de l'Institut Fourier*, 44, 1994.
- [Cou94b] J.-M. Couveignes. Computing isogenies in small characteristic. Submitted for publication, 1994.
- [Cou94c] J.-M. Couveignes. Existence de fonctions de Belyi sans automorphismes. Submitted for publication, 1994.
- [Cou94d] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. Thèse de doctorat, École Doctorale de Bordeaux, 1994.
- [Cré93] C. Crépeau. Cryptographic primitives and quantum theory. In *Proceedings of the second Physics of Computation Workshop, PHYSCOMP'92*, pages 200–204, 1993.
- [Cré94] C. Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.
- [CS91a] Crépeau C and M. Sántha. On the reversibility of oblivious transfer. In *Advances in Cryptology: Proceedings of EUROCRYPT'91*, volume 547 of *LNCS*, pages 106–113. Springer-Verlag, 1991.
- [CS91b] C. Crépeau and M. Sántha. Efficient reductions among oblivious transfer protocols based on new self-intersecting codes. In *Sequences II, Methods in Communications, Security, and Computer Science*, pages 360–368. Springer-Verlag, 1991.
- [CS95] C. Crépeau and L. Salvail. Quantum oblivious mutual identification. In *Advances in Cryptology: Proceedings of Eurocrypt'95*. Springer-Verlag, 1995. à paraître.

- [CSV94] D. Coppersmith, J. Stern, and S. Vaudenay. Attacks on the birational permutation signature schemes. In D. R. Stinson, editor, *Advances in Cryptology CRYPTO'93*, volume 773 of *LNCS*, pages 435–443. Springer-Verlag, 1994. Disponible comme LIENS-93-25.
- [CT95] C. Crépeau and A. Tapp. Committed oblivious transfer. In *Advances in Cryptology: Proceedings of Crypto'95*. Springer-Verlag, 1995.
- [CV94] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In A. de Santis, editor, *Advances in Cryptology: Proceedings of EUROCRYPT'94*. Springer-Verlag, 1994. Disponible comme LIENS-94-3.
- [FJR⁺94] J. Friedman, A. Joux, Y. Roichman, J. Stern, and J.-P. Tillich. Most regular graph are quickly r -transitive. 1994. non-publié.
- [Gra94] L. Granboulan. Construction d'une extension régulière de $Q(T)$ de groupe de galois M_{24} . *Journal of Experimental Maths*, 1994. Submitted for publication.
- [GS94] M. Girault and J. Stern. On the length of cryptographic hash-values used in cryptographic identification scheme. In *Advances in Cryptology, Proceedings of CRYPTO'94*, *LNCS*. Springer-Verlag, 1994.
- [JG94] A. Joux and L. Granboulan. A practical attack against knapsack based hash functions. In *Advances in Cryptology: Proceedings of EUROCRYPT'94*, *LNCS*. Springer-Verlag, 1994.
- [Jou93a] A. Joux. A fast parallel lattice reduction algorithm. Submitted to Gauss Symposium, 1993.
- [Jou93b] A. Joux. *La Réduction des Réseaux en Cryptographie*. Thèse de doctorat, Ecole Polytechnique, 1993. Disponible comme LIENS-93-7.
- [JS91a] A. Joux and J. Stern. Cryptanalysis of another knapsack cryptosystem. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology: Proceedings of ASIACRYPT'91*, volume 739 of *LNCS*, pages 470–476. Springer-Verlag, 1991.
- [JS91b] A. Joux and J. Stern. Improving the critical density of the lagarias-odlyzko attack against subset sum problems. In L. Budach, editor, *Proceedings of Fundamentals of Computation Theory 91*, volume 529 of *LNCS*, pages 258–264. Springer-Verlag, 1991.
- [JS94] A. Joux and J. Stern. Lattice reduction: a toolbox for the cryptanalyst. *Journal of Cryptology*, 1994. soumis au J. Cryptology.
- [LC94] P. Hoogvorst L. Caudal, H. Gilbert. A new identification scheme based on the three dimensional matching problem. non publié, 1994.

- [LS91] G. Lachaud and J. Stern. Polynomial-time construction of linear codes with almost equal weights. In A. de Santis, editor, *Sequences II, Methods in Communications, Security, and Computer Science*, pages 59–62, New York, 1991. Springer-Verlag.
- [LS92a] G. Lachaud and J. Stern. Polynomial-time construction of codes I: linear codes with almost equal weights. *Applicable Algebra in Engineering, Communication and Computing*, pages 151–161, 1992.
- [LS92b] G. Lachaud and J. Stern. Polynomial-time construction of spherical codes. In *Proceedings of the AAECC-9 Conference*, volume 539 of *LNCS*, pages 218–223. Springer-Verlag, 1992.
- [LS94] G. Lachaud and J. Stern. Polynomial-time construction of codes II: Spherical codes and the kissing number of spheres. *IEEE Transactions on Information Theory*, 40:1140–1146, 1994.
- [MNRV94] D. M’Raïhi, D. Naccache, D. Raphaeli, and S. Vaudenay. Complexity trade-offs with the digital signature standard. In A. de Santis, editor, *Advances in Cryptology: EUROCRYPT’94*, 1994. To appear.
- [Poi95] D. Pointcheval. A new identification scheme based on the perceptrons problem. In L. Guillou, editor, *Advances in Cryptology EUROCRYPT’95*, LNCS. Springer-Verlag, 1995. to appear. LIENS-95-2.
- [SBM93] J. Stern, S. Blackburn, and S. Murphy. Weaknesses of a public key cryptosystem based on factorization of finite groups. In T. Helleseth, editor, *Advances in Cryptology: Proceedings of EUROCRYPT’93*, volume 765 of *LNCS*, pages 50–54. Springer-Verlag, 1993.
- [Ste93a] J. Stern. Approximating the number of error locations is NP-complete. In T. Mora, editor, *Proceedings of the AAECC-10 Conference*, volume 673 of *LNCS*, pages 323–331. Springer-Verlag, 1993.
- [Ste93b] J. Stern. A new identification scheme based on syndrome decoding. In *Advances in Cryptology, Proceedings of CRYPTO’93*, volume 773 of *LNCS*, pages 13–21. Springer-Verlag, 1993.
- [Ste94] J. Stern. Designing identification scheme with keys of short size. In *Advances in Cryptology, Proceedings of CRYPTO’94*, volume 839 of *LNCS*, pages 164–173. Springer-Verlag, 1994.
- [SV94a] C. P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In A. de Santis, editor, *Advances in Cryptology: EUROCRYPT’94*, 1994. To appear.
- [SV94b] C. P. Schnorr and S. Vaudenay. Parallel FFT-hashing. In R. Anderson, editor, *Fast Software Encryption, Cambridge Security Workshop*, volume 809 of *LNCS*, pages 149–156. Springer-Verlag, 1994.

- [Vau93a] S. Vaudenay. FFT-Hash-II is not yet collision-free. In E. F. Brickell, editor, *Advances in Cryptology CRYPTO'92*, volume 740 of *LNCS*, pages 587–593. Springer-Verlag, 1993. Disponible comme LIENS-92-17.
- [Vau93b] S. Vaudenay. One-time identification with low memory. In P. Camion, P. Charpin, and S. Harari, editors, *EUROCODE'92*, volume 339 of *CISM Courses and Lectures*, pages 217–228. Springer-Verlag, 1993. Disponible comme LIENS-92-22.
- [Vau95] S. Vaudenay. On the need for multipermutations: Cryptanalysis of MD4 and SAFER. In B. Preneel, editor, *Proceedings of Leuven Workshop on Cryptographic Algorithms*, 1995.