

Rapport de Recherche

Groupe de Recherche en Complexité et Cryptographie

20 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 NP-complets	2
2.2	Théorie algorithmique des nombres: Factorisation des nombres entiers	3
2.3	Algorithmique sur les réseaux à coordonnées entières.	3
2.4	théorie des codes	4
2.5	Analyse cryptographique	4
2.6	Protocoles cryptographiques	5
2.7	Fonctions de Condensation	5
2.8	Procédés d'identification	5
2.9	Cryptographie quantique	6
3	Missions et invitations du GRECC	6
3.1	Invitations	6
4	Diffusion de la Recherche	6
5	évaluation de la Recherche	7
6	Activités d'enseignement	7

1 Composition du groupe

- Responsable: Jacques Stern (Directeur de Recherche au CNRS)
- Membres
 - Claude Crépeau (Chargé de Recherche au CNRS)

- Antoine Joux (Thésard (J. Stern) ingénieur de l’armement)
- Jean Marc Couveignes (Thésard (J. Stern) ingénieur de l’armement)
- Serge Vaudenay (Thésard (J. Stern) élève à l’Ecole Normale Supérieure)
- Louis Granboulan (Thésard (J. Stern) élève à l’Ecole Normale Supérieure)
- Ludovic Caudal (Thésard (J. Stern) élève à l’Ecole Normale Supérieure de Cachan)

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 ont été perçus par le Laboratoire comme le soutien des instances du CNRS au développement de ce groupe. Le responsable du GRECC devant succéder à Claude Puech comme professeur détaché à l’ENS, à partir d’octobre 1993, la pérennité du groupe paraît maintenant établie.

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.

2.1 Théorie de la complexité: Preuves Interactives et Approximation des problèmes 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 clés publiques (où la clé 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, SAS93]).

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, SAS93]).

2.2 Théorie algorithmique des nombres: 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 pour factoriser des nombres *spéciaux* de la forme $a^b \pm c$ 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 ([?]) 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.

2.3 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, Lovasz, 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 Belle 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.

Le groupe a également utilisé l'algorithme LLL pour calculer explicitement des objets mathématiques complexes: les revêtements de la sphère ramifiés au dessus de trois points seulement. 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 ([Cou93]).

2.4 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 [CS91b] [CS91a].
- 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 meilleurs 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, LS93]).

Enfin, les codes interviennent à plusieurs reprises dans la construction de protocoles basés sur les phénomènes quantiques [BBCS92] [BCJL93].

2.5 Analyse cryptographique

L'analyse cryptographique est la partie de la cryptographie qui s'efforce de recouvrir 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 Lovász (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 ([Ste93c]).

2.6 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 $f(a, b)$.

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.

2.7 Fonctions de Condensation

L'un des problèmes pratiques que rencontre la cryptographie est la définition de fonctions de condensation (ou de hachage) associant à un (long) message un condensé de quelques centaines de bit. Cette opération doit se faire de façon qu'il soit virtuellement impossible de calculer deux messages ayant même condensé. Le GRECC a ainsi étudié la fonction de hachage FFT-Hash 2 proposée par Claus Schnorr au colloque EUROCRYPT'92 (Hongrie, mai 1992) pour laquelle il a trouvé des collisions ([?]). 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 ([?]).

2.8 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 un protocole d'identification fondé sur la mise en œuvre de codes correcteurs d'erreurs ([Ste93b]).

2.9 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 [BBCM93] [BCJL93]. Le GRECC a enfin participé à des recherches de physique fondamentale sur la téléportation d'un état quantique [BBC⁺93].

3 Missions et invitations du GRECC

3.1 Invitations

- Visite d'Adi Shamir (Weizmann Institute), février 1992-juillet 1992.
- Visite de Claus Schnorr (Université de Francfort), avril 1993

4 Diffusion de la Recherche

- Organisation à l'Ecole Normale Supérieure, d'un séminaire régulier. Parmi les conférenciers récents: J.J. Quisquater (Philips), A. Shamir (Weizmann), J. Friedman (Princeton), C. Schnorr (Francfort), P. Landrock (Aarhus), U. Maurer (ETH, Zurich).

- 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 Cargese d'une réunion des participants à l'appel d'offre des PRC Codage, complexité et cryptographie.

5 evaluation de la Recherche

- C. Crépeau: membres du comité éditorial du Journal of Cryptology depuis 1991.
- J. Stern: membre du comité de programme d'Eurocrypt '92 et Eurocrypt '94; membre du comité de programme d'Eurocode 92; membre du comité de programme de ACM Conference on Computer and Communications Security 1993.

6 Activités d'enseignement

- MMFAI: J. Stern, A. Joux.
- Maîtrise d'Informatique Orsay: C. Crépeau
- ENSTA 3ème année: C. Crépeau, A. Joux
- filière Algorithmique, Complexité et Cryptographie du du DEA d'Informatique mathématique (IMA): J. Stern, C. Crépeau.

Références

- [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.
- [BBCM93] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Privacy amplification against Probabilistic Information. *IEEE Transaction on Information Theory*, 1993. submitted for publication.
- [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.
- [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.
- [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*, pages –, 1993.
- [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*, LNCS. Springer-Verlag, 1993. To appear.
- [Cou93] J.-M. Couveignes. Calcul et rationalité de fonctions de belyi en genre 0. soumis aux annales de l'Institut Fourier, 1993.
- [Cré93] C. Crépeau. Cryptographic primitives and quantum theory. In *Proceedings of the second Physics of Computation Workshop, PhysComp '92*, pages 200–204, 1993.
- [CS91a] 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.
- [CS91b] C. Crépeau 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.

- [Jou93a] A. Joux. A fast parallel lattice reduction algorithm. Soumis au Gauss Symposium, 1993.
- [Jou93b] Antoine Joux. *La Réduction des Réseaux en Cryptographie*. Thèse de doctorat, Ecole Polytechnique, 1993. Prépublication, rapport LIENS-93-7.
- [JS91a] A. Joux and J. Stern. Cryptanalysis of another knapsack cryptosystem. In *Advances in Cryptology: Proceedings of AsiaCrypt'91*, LNCS. 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.
- [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 —, 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.
- [LS93] G. Lachaud and J. Stern. Polynomial-time construction of codes ii: Spherical codes and the kissing number of spheres. *IEEE Transactions on Information Theory*, 1993.
- [SAS93] J. Stern S. Arora and Z. Sweedyk. The hardness of approximating problems defined by linear constraints. 1993. submitted to FOCS '93.
- [Ste93a] J. Stern. Approximating the number of error locations is np-complete. In T. Mora, editor, *Proceedings of the AAECC-10 Conference*, LNCS. Springer-Verlag, 1993.
- [Ste93b] J. Stern. A new identification scheme based on syndrome decoding. 1993. submitted to Crypto '93.
- [Ste93c] J. Stern. Weaknesses of a public key cryptosystem based on factorization of finite groups. In T. Helleseth, editor, *Avances in Cryptology: Proceedings of Eurocrypt '93*, LNCS. Springer-Verlag, 1993.