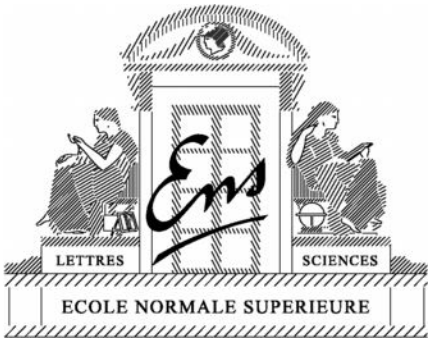

Département d'Informatique de l'École Normale Supérieure

Rapport scientifique

(1998-2001)

Table des matières

Message du directeur

A l'automne 1999, l'Ecole normale supérieure, conjuguant sa tradition bidentenaire et sa capacité d'innovation, a créé le Département d'informatique (DI). Quinze ans environ après la création du DMI (Département de mathématique et d'informatique), il est apparu que l'autonomie des thèmes de recherche en informatique et la nécessité de répondre au défi que constitue la formation d'informaticiens de haut niveau nécessitaient que l'ENS se dotât d'un nouveau département.

L'autonomie ainsi acquise offre de nouvelles possibilités : :

- accueil au sein du DI d'autres équipes et chercheurs, notamment venant de l'INRIA
- meilleure articulation entre recherche et enseignement

A côté des cinq équipes regroupées dans une Unité Mixte de Recherche CNRS-ENS, le DI a pu accueillir un projet commun INRA-CNRS, ce qui a permis de développer un nouveau thème de recherche et de d'élargir de spectre de l'informatqiue présenté aux élèves de l'Ecole.

La création du DI, par la séparation en deux entités de l'ancien DMI (Département de mathématiques et informatique) s'est faite dans de bonnes conditions. Toutefois, le projet scientifique qui la sous-tend est loin d'être mené à terme. Pour progresser, l'ensemble des membres du département a mené un effort de réflexion, notamment au cours d'un séminaire hors des murs de l'Ecole. Un conseil scientifique du département, réuni les 8 et 9 décembre 2000, nous a également aidé à préciser nos ambitions et à identifier les difficultés qu'il nous fallait surmonter. Ce conseil a estimé que le DI avait vocation à devenir un "leader mondial de qualité comparable aux meilleurs départements américains". Pour y parvenir, il a préconisé une croissance accélérée sur cinq ans, un élargissement des thèmes de recherche et un rééquilibrage de l'enseignement.

Une croissance accélérée La principale faiblesse du DI est à l'évidence sa taille. Au sein du LIENS, il n'y a pour l'instant que sept enseignants-chercheurs de l'ENS, quatre collègues du CNRS et deux de l'INRIA. Cette situation, qu'on peut qualifier de critique, est la conséquence d'un certain nombre de facteurs :

- Le faible nombre de postes à l'ENS.
- La modestie du nombre des recrutements dans les années récentes.
- La redéfinition de nos thèmes de recherche : l'existence d'un département commun aux mathématiciens et aux informaticiens avait conduit naturellement à une sur-représentation de l'informatique théorique, voire à la présence de chercheurs dont la pratique relèvait presque exclusivement des mathématiques.
- La règle de fonctionnement singulière dite «règle des dix ans», imposée par les mathématicients et qui limite à dix années la durée maximale pendant laquelle un chercheur ou un enseignant-chercheur de cette discipline, peut demeurer à l'ENS. Cette règle a aussi provoqué plusieurs départs. Le DI, tout en étant attaché à la mobilité, ne la reconnaît pas.

La situation est aujourd'hui propice à la définition d'objectifs ambitieux : le gouvernement a fait du développement des sciences et technologies de l'information et de la communication (STIC) une priorité nationale ; la nouvelle direction du CNRS a créé un département STIC, qui a été doté, dès cette année, d'un nombre significatif de créations de postes ; enfin l'INRIA, dont le nombre de chercheurs augmente fortement, entend s'ouvrir vers la recherche universitaire. Le doublement de notre capacité de recherche dans les cinq prochaines années nous est donc apparu comme un objectif mobilisateur. Un tel objectif nécessite un effort de la part de tous les partenaires concernés. On attend :

- que l'ENS obtienne rapidement la création d'un poste de maître de conférences ainsi que celle d'un poste de professeur associé, sur lequel pourrait être recrutée une personnalité du milieu industriel
- que le CNRS poursuive au niveau national l'effort commencé en 2000 et qu'il prenne en compte la spécificité du LIENS, par exemple par des postes fléchés
- que l'INRIA développe le partenariat initié avec la mise à disposition de François Baccelli

Un élargissement des thèmes de recherche Il s'agit là de la poursuite d'un objectif intimement lié à la création du DI et qui a déjà été au centre de nos préoccupations dans les précédentes années. Comme on l'a déjà dit, l'environnement d'un département commun avec les mathématiciens conduisait naturellement au développement de thèmes relevant de l'informatique fondamentale : sémantique et algorithmique. Sans renoncer à ce positionnement amont dans la discipline, le Laboratoire a su développer, organiser et renouveler des groupes thématiques actifs et, pour la plupart, ouverts aux collaborations et aux applications. Ce modèle "vertical", allant de la théorie aux applications, n'a pas vocation à être uniformément imposé mais, pour les équipes qui ne l'adoptent pas pleinement, l'heure est à la cohésion et la restructuration plus qu'à la croissance.

Il va de soi que le doublement d'un Laboratoire, ne peut se faire par simple "homothétie". Si les thèmes de recherche les moins nombreux doivent augmenter leurs effectifs, la nécessité de nouveaux thèmes, en phase avec les enjeux de l'informatique moderne est évidente pour tous. Parmi les champs d'application à explorer, la bio-informatique s'impose : les problèmes de génomique sont, à bien des égards, de nature informatique. On peut également citer d'autres domaines d'application d'un grand intérêt à l'heure actuelle

- grandes bases de données
- "data mining"
- réalité virtuelle et modélisation 3D

Enseignement et recherche Un département établi à l'Ecole normale ne peut définir sa stratégie indépendemment de l'institution qui l'héberge. Le DI a évidemment l'ambition d'attirer vers la discipline informatique une partie des élèves de l'École et d'irriguer ainsi, à l'image de ce qui se fait en mathématiques, en physique, en philosophie, en lettres et dans d'autres spécialités, les universités et les institutions de recherche du pays. Il s'agit de montrer la richesse et la diversité de la pratique de la recherche en insistant sur la spécificité de l'informatique : présence de nombreux doctorants dans les laboratoires, importance des applications, relations contractuelles nombreuses avec des partenaires institutionnels ou privés. Là encore, le handicap du département d'informatique est sa taille. A l'objectif du doublement des effectifs des chercheurs s'ajoute donc naturellement l'objectif du doublement du nombre d'élèves. Ce doublement ne se fera pas sans changement dans l'organisation du concours d'entrée. Le DI souhaite, aussi rapidement que possible, la mise en place d'un concours séparé, doté d'un nombre significatif de places et commun avec l'ENS-Lyon qui a anticipé cette évolution.

Avant de conclure, il convient de présenter brièvement le rapport qui suit. En se reportant au bilan scientifique, on constatera que le DI continue à avoir un taux élevé de publications de très haut niveau, plusieurs centaines depuis 1997. On pourra également noter la poursuite de collaborations internationales nombreuses et d'une activité contractuelle importante : participation à plusieurs projets européens, contrats avec des partenaires publics ou privés, organisation de nombreuses manifestations scientifiques etc. C'est ainsi que le montant des ressources contractuelles a atteint un niveau significatif.

A côté de ces éléments positifs, on trouve des sujets d'inquiétude, notamment l'évolution des effectifs du département en ce qui concerne l'équipe d'administration. Cette année, elle est réduite à deux personnes (une affectée par le CNRS et une par l'ENS). Il faut rendre hommage au dévouement de cette équipe mais la situation n'est plus tenable. Chaque institution s'est heureusement engagée mettre à la disposition du DI une personne supplémentaire.

Le bilan est également préoccupant pour les chercheurs, alors même que

le Laboratoire vise un accroissement notable. Il y a eu exactement quatre départs et quatre arrivées dans les quatre dernières années. Nous attendons beaucoup du CNRS et de l'INRIA pour redresser cette orientation extrêmement négative.

L'École normale supérieure joue, dans le paysage universitaire français un rôle particulier, par la qualité de ses élèves et de ses laboratoires. L'informatique est aujourd'hui l'un des moteurs de l'innovation scientifique et technique. Pourtant, elle n'a pas encore, à l'Ecole, la place qu'elle devrait avoir. Compte tenu de l'engagement clair pris par le gouvernement de favoriser le développement des STIC, la période qui s'ouvre est un moment privilégié pour donner une meilleure visibilité à l'informatique. Il est possible de doubler la taille du département. Il est possible de changer le concours d'entrée. Il est possible aussi de décider d'affecter au DI des locaux propres, à la mesure du rôle qu'on veut lui voir jouer. L'ENS pourra ainsi relever le défi : devenir l'un des centres d'excellence en informatique, au niveau mondial.

Paris, le 15 mars 2001,

Jacques Stern

Architectures et algorithmes matériels

Composition de l'équipe

- Responsable :
  Jean Vuillemin, professeur à l'ENS ;
- Membres permanents :
  Mark Shand, *consulting engineer* détaché de *Compaq - System Research Center (Palo-Alto – USA)* ;
  Laurent Moll, chercheur, 1998-2001.

Thèmes de recherche

Notre recherche est motivée par la réalisation effective de systèmes digitaux à très haute performance. Les applications viennent de domaines variés : de la physique des hautes énergies à l'imprimerie, en passant par l'astronomie solaire et la cryptographie. Les techniques utilisées sont à cheval sur le matériel et le logiciel, les algorithmes, l'arithmétique et l'architecture.

Le groupe est pionnier reconnu du système re-configurable : c'est un ordinateur hybride, dont une partie des composants - FPGA - est programmable. Ceci permet de réaliser un nombre arbitraire de circuits (et systèmes) performants sur un matériel unique. L'acquis (industriel) initial sur le sujet est présenté dans [3] - *prix IEEE Circuits and Systems Society 1998 VLSI Transactions Best Paper Award, et meilleur "quotation index" du domaine.* Nous détenons (par exemple) depuis 92 les records absolus de vitesse pour la cryptographie RSA, tout matériels confondus pour une version, et tous logiciels pour l'autre. Les (nombreux) algorithmes arithmétiques (programmes et circuits) utilisés sont décrits en [16] - ils restent inchangés à ce jour. Pour cette application et les autres, la clé du succès réside dans une intégration étroite entre la spécification de l'algorithme et sa mise en oeuvre par le système - programmes et circuits.

Nos recherches portent sur quatre sujets : les applications, l'architecture matérielle de systèmes re-configurables, les logiciels système et de synthèse de logique associés et la théorie qui permettrait automatiquement de mesurer, d'optimiser et de vérifier des systèmes aussi complexes.

1 Applications

1.1 Astronomie solaire

Une collaboration fructueuse existe avec la section de la *Royal Swedish Academy of Sciences* qui dirige l'observatoire solaire des îles Canaries : [6] [14] [2] [21]. Il est dit (publiquement) que le système d'acquisition d'images réalise avec Pamette est l'une des contributions techniques majeures à astronomie solaire, depuis vingt ans. Aujourd'hui, il faut contrôler en temps réel l'optique adaptative du télescope : [15] [1].

1.2 Composition de vidéo

Un réseau de Pamette permet de composer en *une seule image* des vidéos synthètiques partielles issues de chaque machine d'un gros cluster [9]. Ce système Sepia est la base d'une proposition de Compaq à ASCI/VIEWS qui vise à la réalisation de systèmes capables de simuler et de visualiser des *expériences virtuelles* de grande taille et durée.

1.3 Mesure de performance en temps réel

Pamette est un instrument incomparable pour la mesure (et la mise au point) des systèmes complexes : on peut lui faire " espionner " ce qu'on veut, comme les bus des nouvelles machines. C'est mis en œuvre chez Compaq [10] et le caractère inattendu de certaines mesures conduit à des variations nouvelles sur les protocoles de Bus [20].

1.4 Réseau de capteurs

Un thème nouveau est l'utilisation de réseaux de capteurs DAM - audio pour le moment - pour explorer de nouvelles techniques dans la détection d'origine et le filtrage de sources audio multiples. Des expériences sur le dé-multiplexage en continu de sources audio DAM sont en cours.

2 Matériels réalisés

Pour des raisons évidentes, ces réalisations se font dans un cadre industriel externe à l'Ecole : Compaq et Hewlett-Packard.

2.1 PCI-Pamette

Pamette est un système re-configurable de petite taille, conçu pour faire du traitement à la volée de données externes à forte bande passante. Plusieurs centaines de systèmes sont utilisés dans le monde industriel et des grands centres de recherche. Pamette est utilisé à l'Ecole Normale ainsi qu'à Polytechnique pour des cours sur la réalisation effective de système matériel.

2.2 CHESS

En collaboration avec les laboratoires HP de Bristol et de Palo-Alto, nous avons conçu et réalisé le circuit CHESS. C'est le premier (six brevets en cours) *Dynamically Programmable Arithmetic Array DPAA* d'une nouvelle génération de composants. La publication [7] en décrit le détail, et montre que la densité de calcul obtenue par CHESS est 10 fois celle d'un FPGA, pour les opérateurs de base en traitement du signal, la compression JPEG, ainsi que le rendu des images en demi-teinte - pour l'imprimerie.

3 Outils et langages de description de systèmes synchrones

3.1 PAM-DC

Pour suivre les évolutions conjointes de la complexité des applications et celle des circuits re-configurables, il a fallu adapter en continu les outils de synthèse de circuits issus de [3] et intégrer un logiciel run-time pour Pamette [12]. Les outils JHDL (Brigham Young University) s'en inspirent.

3.2 Jazz

Une tentative de fonder un langage de description de circuits sur des principes plus fondamentaux est en cours avec l'Ecole des Mines (Berry, Frey, Bourdoncle). C'est le langage Jazz, utilisé pour l'enseignement à l'Ecole Normale.

4 Théorie des circuits

4.1 Analyse et synthèse de circuits

Nous travaillons sur une technique d'analyse et de représentation des circuits par leur table de vérité, qui est racine d'un 2- polynôme fini et caractéristique du circuit [5].

4.2 Densité de calcul

Une théorie de la densité de calcul est reprise en [4], à propos de CHESS. Il s'agit de quantifier la question : *Combien d'opérations binaires peut-on calculer, par micron carré (de silicium) et nano seconde ?* L'architecture de machines optimisées pour la densité de calcul est un sujet industriel important pour les fabricants d'ordinateurs, de composants comme de systèmes : tout gain de densité réduit d'autant le coût unitaire de production.

Éléments d'évaluation

1 Collaborations

- Collaborateurs réguliers.
  - Laurent Moll, chercheur dans l'équipe de 98 en 00.
  - Patrice Bertin, École des Mines.
  - Göran Sharmer, membre de la Royal Swedish Academy of Sciences, Suède.
  - Gérard Berry, Esterel Technologies, France.
  - David Skellern, professeur à Macquarie University, Australie.
  - Brad Hutchings, professeur à Brigham Young University, USA.
  - Alan Marshall, HP Laboratory de Bristol, UK.
- Collaborations industrielles.
  - En accord avec Compaq, participation de Mark Shand aux recherches et à l'enseignement du Département, depuis 98.
  - Jean Vuillemin était "visiting scholar" pour HP-Laboratories, de 96 à 99.
  - Le groupe donne des "conseils en brevets" pour Mentor-Graphics. Ceci a fait l'objet de deux contrats en 99 et 00.

2 Missions, conférences et séminaires

- Jean Vuillemin (conférences invité) :

  98 HP-Laboratories, Stanford EE Colloquium (Palo Alto, USA – février), CAVE workshop (Linkoping, Suède – mai), VECPAR'98 (Porto, Portugal – juin), HP keynote (Bristol, UK – novembre).

  99 HP award lecture (Bristol, UK – janvier), ISIA (Sophia-Antipolis – octobre), Imperial College (Londres, UK – octobre), séminaire algo (INRIA, Rocquencourt – novembre), ASIAN'99 (Phuket, Thailand – décembre).

  00 Université de Caen – mars, Chalmer's lecture (Goeteborg, Suède – mai), Keynote speaker VECPAR'2000 (Porto, Portugal – juin), Keynote Talk ASIAN'00 (Penang, Malaisie – novembre), ;

01 séminaire algo (INRIA, Rocquencourt – mars), CREST lecturer (Atlanta, USA – mars), lecture (Chalmers, Suède – mai).

- Mark Shand :

  00 FCCM'00 (Napa, USA – avril), Caltech CNSE (Los Angeles, USA – mai), Dagsthul 261 (Allemagne – juin), Hotchips (Stanford, USA – aout), Supercomputing (Dallas, USA – novembre), Xilinx symposium (Paris – novembre).

3 Accueil de chercheurs

Visites du groupe pour moins de 8 jours par 17 chercheurs internationaux en 2000.

4 Diffusion de la connaissance

Diverses notes de cours à Polytechnique et à l'ENS.

5 Réalisation et diffusion de logiciels, brevets

- M. Shand : brevet sur les protocoles de bus [20].
- M. Shand : brevet sur un outil de filtrage reconfigurable [21].
- M. Shand : brevet sur un circuit de mémoire avec dispositif de réinitialisation [19].
- Le travail sur CHESS [7] fait l'objet de 6 dépots de brevets par Jean Vuillemin et d'autres : [23],[27],[26],[22],[25],[24].
- Le logiciel Jazz, réalisé en commun avec l'Ecole des Mines, est dans le domaine public, et il est utilisé pour l'enseignement à l'ENS et à l'ISIA.

6 Participations à l'évaluation de la recherche

- J. Vuillemin :

  Membre du jury senior de l'Institut Universitaire de France : 98-99.

  Président de la Commission de spécialistes ENS, section 27 : 97- .

  Vice-président du Concours ENS pour l'Informatique : 00- .

  Membre du comité de rédaction de : Acta Informatica (Sringer Verlag). Journal of Algorithms (Academic Press). Journal of VLSI and Computer Systems (Computer Science Press). The International Series of Monographs on Computer Science (Oxford University Press). Integration The VLSI Journal (North Holland). Foundations of Computer Science (World scientific). Journal of VLSI Signal Processing (Kluwer Academic Publishers).

– M. Shand :
  Membre du comité de programme de FCCM : *Field-Programmable Custom Computing Machines.*

  Consulting engineer pour Compaq.

7 Encadrement doctoral

Participation à des jurys de thèses
– J. Vuillemin : 12 jurys, 3 rapports.
– M. Shand : 3 jurys.

Encadrement de stages
– M. Shand.
  Stages pour 7 élèves ENS, mars/juin 99.

  Stage pour 2 élèves de Polytechnique, sur une interface pour le *Swedish Vaccuum Solar Telescope*, Paris, Stockholm, Las Palma (Canaries) – mai, juillet 00.

  Stages pour 2 élèves ENS, cryptographie Rinjdeal, mars/juin 00.

  Stage pour 2 élèves ENS, acquisition d'image, octobre 00/février 01.

8 Enseignement

Deuxième cycle
– J. Vuillemin
  Cours de "Théorie de l'Information", MMFAI 1-ere année (depuis 98).

  Cours "Systèmes Reconfigurables", MMFAI 2-ième année (depuis 98).

  Majeure "Algèbre et Informatique", École Polytechnique (jusqu'en 01).
– M. Shand
  Cours "Systèmes Reconfigurables", MMFAI 2-ième année (depuis 98).

Troisième cycle
– J. Vuillemin
  Cours *Circuits* du DEA Sémantique de Paris (en 02).

9 Prix et distinctions

Notre publication [3] a obtenu le prix *IEEE Circuits and Systems Society 1998 VLSI Transactions Best Paper Award.*

Équipe Architectures et algorithmes matériels

De 95 à 99, Jean Vuillemin a été l'un des trois *consulting scholar* auprès de HP-Laboratories ; les deux autres étaient Abraham Lempel et David Skellern.

Publications

Articles dans des revues internationales avec comité de lecture

[1] G. B. Scharmer, M. Shand, M. G. Löfdahl, P. M. Dettori et W. Wei. – A workstation based solar/stellar adaptive optics system. *Adaptive Optical Systems Technologies*, vol. 4007, 2000, pp. 239–250.

[2] M. Shand et G. Scharmer. – The swedish vacuum solar telescope data acquisition and control systems. *New Astronomy Reviews*, vol. 42, 1998, pp. 481–484.

[3] J. Vuillemin, P. Bertin, D. Roncin, M. Shand, H. Touati et P. Boucard. – Programmable active memories : the coming of age. *IEEE Trans. on VLSI*, vol. 4, NO.1, March 1996, pp. 56–69.

Conférences invitées

[4] J. Vuillemin. – Re-configurable systems : Past and next 10 years. *In : Vector and Parallel Processing - VECPAR'98. Lecture Notes in Computer Science*, vol. 1573, pp. 334–354. – Springer-Verlag, 1998. (invited talk).

[5] J. Vuillemin. – Finite circuits are characterized by 2-algebraic truth-tables. *In : ASIAN'00 Computing. Lecture Notes in Computer Science.* – Springer-Verlag, 2000.

Communications dans des conférences internationales avec comité de lecture

[6] J. S. Almeida, M. Collados, V. M. Pillet, V. G. Escalera, G. B. Scharmer, M. Shand, L. Moll, E. Joven, A. Cruz, J. J. Diaz, L. F. Rodriguez, J. Fuentes, L. Jochum, E. Paez, B. Ronquillo, J. M. Carranza et I. Escudero-Sanz. – The IAC solar polarimeters : Goals and review of two ongoing projects. *In : Advances in Physics of Sunspots, ASP Conf. Ser. : 1st Advances in Solar Physics Euroconference*, vol. 118, p. 366. – 1997.

[7] A. Marshall, J. Vuillemin, T. Stansfield, I. Kostarnov et B. L. Hutchings. – A re-configurable arithmetic array for multimedia applications. *In : Proceedings of the 1999 ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, pp. 135–143. – 1999.

[8] T. McDermott, P. Ryan, M. Shand, D. Skellern, T. Percival et N. Weste. – A wireless lan demodulator in a pamette : Design and experience. *In : FPGAs for Custom Computing Machines (FCCM'97)*, éd. par K. L. Pocek et J. M. Arnold. – IEEE Computer Society Press, April 1997.

[9] L. Moll, A. Heirich et M. Shand. – Sepia : scalable 3D compositing using PCI pamette. *In : In IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'99)*, éd. par K. L. Pocek et J. M. Arnold. – IEEE Computer Society Press, April 1999.

[10] L. Moll et M. Shand. – Systems performance measurement on PCI pamette. *In : FPGAs for Custom Computing Machines (FCCM'97)*, éd. par K. L. Pocek et J. M. Arnold. – IEEE Computer Society Press, April 1997.

[11] M. Shand. – A case study of algorithm implementation in reconfigurable hardware and software. *In : 7th International Workshop on Field Programmable Logic, FPL '97. Lecture Notes in Computer Science.* – Springer-Verlag, September 1997.

[12] M. Shand. – Infrastructure of PCI pamette. *In : Dynamically Reconfigurable Architectures*, *Dagsthul seminar*, n°00261. – 2000.

`http://www.dagstuhl.de/`.

[13] M. Shand. – The Von Neumann bottleneck and other myths. *In : Dynamically Re-configurable Architectures*, *Dagsthul seminar*, n°00261. – 2000.

`http://www.dagstuhl.de/`.

[14] M. Shand et L. Moll. – Hardware/software integration in solar astronomy. *In : IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'98)*, éd. par K. L. Pocek et J. M. Arnold. – IEEE Computer Society Press, April 1998.

[15] M. Shand, G. B. Scharmer et W. Wei. – Correlation tracking and adaptive optics control using off-the-shelf workstation technology. *In : High Resolution Solar Physics : Theory, Observations and Techniques, Proc. 19th Sacramento Peak Summer Workshop*, éd. par R. R. R. T. Rimmele et K. S. Balasubramaniam, *ASP Conf. Series*, vol. 183, p. 231. – 1999.

[16] M. Shand et J. Vuillemin. – Fast implementation of RSA cryptography. *In : 11-th IEEE Symposium on Computer Arithmetic.* – 1993.

Rapports de recherche

[17] O. Mencer, M. Shand et M. J. Flynn. – *Firelink : A re-configurable firewire testbed.* – Rapport technique n° Technical Note 1998-012, Palo Alto, CA, Digital Systems Research Center, June 1998.

Oeuvres de vulgarisation scientifique

[18] J. Vuillemin. – Les langages numèriques. *In : Le langage Scientifique*, éd. par F. Letoublon. – Université de Grenoble, 1998. (invited talk).

Brevets

[19] M. Shand. – Method and apparatus for resetting a random access memory, patent number us6192447, 20 february 2001.

[20] M. Shand. – Method and apparatus for a relaxed bus protocol using heuristics and higher level supervision, patent number us6108734, 22 august 2000.

[21] M. Shand. – Configurable digital signal interface using field programmable gate array to reformat data, patent number us5692159, 25 november 1997.

[22] A. Stansfield, A. Marshall et J.Vuillemin. – Ep00924602a2 : Instruction masking in providing instruction steams to a processor, 06/23/1999.

[23] A. Stansfield, A. Marshall et J.Vuillemin. – Ep00924625a1 : Configurable processor, 06/23/1999.

[24] A. Stansfield, A. Marshall et J.Vuillemin. – Ep01038216a1 : Hierarchical configuration RAM, 08/12/2000.

[25] A. Stansfield, A. Marshall et J.Vuillemin. – Ep01038216a1 : Implementation of multipliers in programmable arrays, 09/27/2000.

[26] A. Stansfield, A. Marshall et J.Vuillemin. – Ep00956645a1 : Field programmable processor, 11/17/1999.

[27] A. Stansfield, A. Marshall et J.Vuillemin. – Ep00956646a1 : Field programmable processor arrays, 11/17/1999.

Complexité et cryptographie

Composition de l'équipe

- Responsable :
  Jacques Stern, professeur à l'ENS ;
- Autres membres permanents :
  Louis Granboulan, maître de conférences à l'ENS depuis sept. 1998 ;
  Phong Nguyen, chargé de recherche CNRS depuis octobre 2000 ;
  David Pointcheval, chargé de recherche CNRS depuis octobre 1998 ;
  Serge Vaudenay, chargé de recherche CNRS jusqu'en octobre 1999 ;
- Doctorants :
  Olivier Baudron, allocataire moniteur X, de sept. 98 à sept. 01 ;
  Emmanuel Bresson, ingénieur de l'armement, depuis sept. 99 ;
  Pierre-Alain Fouque, thésard CIFRE, d'octobre 98 à octobre 01 ;
  Gwenaëlle Martinet, CDD NESSIE, depuis sept. 00 ;
  Thomas Pornin, allocataire moniteur, depuis sept. 98 ;
  Guillaume Poupard, ingénieur de l'armement, de sept. 96 à mai 00.

Thèmes de recherche

Créé en 1988, le Groupe de Recherche en Complexité et Cryptographie (GRECC), a été intégré au LIENS en 1993. Depuis cette date de nombreuses thèses ont été soutenues (13 d'ici juin 2001). Le groupe a ainsi joué un rôle majeur dans la diffusion de la recherche en cryptographie dans le milieu académique français.

Plus que la théorie de la complexité, c'est la cryptologie, dans ses aspects théoriques et pratiques qui forme maintenant le cœur des recherches menées au GRECC. Il s'agit d'un domaine très "vertical" puisqu'il va de sujets proches de la complexité abstraite à la conception d'algorithmes cryptographiques, voire à leur implantation sur ordinateur ou sur carte à mémoire. Nombre de questions posées sont directement issues de la pratique et proviennent de divers domaines : commerce électronique, internet, télévision à péage, sécurité des communications GSM ou UMTS notamment.

Dans les quatre dernières années, le GRECC a concentré ses recherches dans les domaines suivants, couvrant la quasi totalité des thèmes actuellement actifs dans la communauté de recherche en cryptologie :

1. Preuves de sécurité pour les schémas de signature
2. Preuves de sécurité pour les schémas à clé publique
3. Authentification mutuelle et échange de clés
4. Nouveaux problèmes difficiles
5. Conception de nouveaux algorithmes à clé publique
6. Cryptanalyse des systèmes à clé publique
7. Cryptanalyse des systèmes symétriques
8. Conception et implantation d'algorithmes symétriques
9. Cryptographie "interactive"

1 Preuves de sécurité pour les schémas de signature

Une tendance significative de la recherche la plus récente en cryptographie vise à substituer aux approches heuristiques une "sécurité prouvée". Le

simple fait qu'un algorithme cryptographique ait résisté durant plusieurs années aux attaques des cryptanalystes a constitué pendant longtemps la seule forme possible de validation. Un paradigme totalement distinct provient du concept de "sécurité prouvée". Cette approche propose des preuves relatives qui ramènent la sécurité du schéma proposé à celle d'un problème mathématique classique difficile à résoudre, tel que la factorisation des entiers ou le problème du logarithme discret. Bien entendu, tout comme dans d'autres sciences, on fait, le cas échéant appel à une certaine idéalisation des objets qu'on manipule. C'est ainsi qu'on identifie souvent les fonctions de hachage à des fonctions aléatoires (modèle de l'oracle aléatoire). A ce prix, on obtient des "preuves" qui ne sont, au plan méthodologique, qu'une technique améliorée de détection des erreurs mais qui contribuent fortement à la confiance.

En utilisant des outils de théorie de la complexité, le groupe a pu dans [10] prouver la sécurité d'une modification mineure du schéma de signature maintenant classique de ElGamal. Nous avons ensuite étudié d'autres variantes de la signature ElGamal [89, 24], dont une a été retenue dans la norme ISO 14888. La méthode a alors été appliquée avec succès au problème de la sécurité des signatures "en blanc", inventées en 1982 par David Chaum dans le but de reproduire sous une forme purement numérique les principales caractéristiques de l'argent liquide, y compris l'anonymat des transactions. Le problème semble naïf : prouver qu'après avoir reçu n pièces de monnaie électroniques, un utilisateur ne peut en générer $n + 1$, mais la question restait, depuis quinze ans, d'ordre conjectural. En systématisant la méthode que nous avions utilisée pour les signatures El Gamal, nous avons pu proposer un schéma de signature en blanc de sécurité prouvée [10]. Nous avons également proposé dans [62] le premier schéma de signature en blanc prouvé équivalent à la factorisation.

Ayant clarifié le mécanisme des preuves de sécurité, le GRECC a cherché à l'appliquer à des environnements où les ressources de calcul sont limitées, l'idée étant d'explorer des stratégies de conception d'algorithmes plus "risquées" en les validant par une preuve. C'est ainsi qu'ont été proposés deux mécanismes de signature à la volée [65, 67], compatibles avec le temps dont peut disposer une carte à microprocesseur sans contact pour effectuer une opération de péage. Par ailleurs, les outils que nous avons introduits nous ont permis des contributions à d'autres domaines pratiques, notamment celui du recouvrement des clés cryptographiques puisque nous avons mis au point le premier système d'encapsulation de clés RSA, muni d'une preuve compacte établissant que les données encapsulées permettent bien la restauration de la clé [68].

Dans le même ordre d'idées mais en cherchant à limiter cette fois la taille des signatures, le groupe a imaginé un schéma adapté au contexte très particulier de l'affranchissement électronique [43] : les services postaux de plusieurs pays envisagent en effet d'utiliser des mécanismes cryptographiques et, là encore, la capacité de produire des preuves permet de valider de sché-

mas réduisant les marges de sécurité pour s'adapter aux performances des lecteurs optiques.

La question des preuves de sécurité peut sembler théorique : selon nous, il n'en est rien. Il s'agit de recherche appliquée. Nos solutions s'inscrivent dans un courant de recherche actif sur les infrastructures de clés publiques (PKI), qui seront sans doute au cœur des applications de la cryptographie dans un proche avenir.

2 Preuves de sécurité pour les schémas à clé publique

En utilisant l'expertise acquise dans le domaine des signatures, le groupe a participé à la clarification des notions de sécurité pour le chiffrement asymétrique, et ce, en collaboration avec des collègues américains [18]. Puis nous avons étudié les notions de sécurité du chiffrement dans un mode multi-destinataires [16].

Nous avons également proposé plusieurs schémas avec des preuves de sécurité [55, 58]. Mais ces travaux étaient spécifiques à chaque schéma. Or, la plupart des schémas à clé publique ont une propriété de sécurité minimale face à une adversaire cherchant seulement à inverser *ex nihilo* un message chiffré. Les exigences de sécurité qu'on met aujourd'hui en avant considèrent des adversaires bien plus puissants, autorisés à obtenir des déchiffrements d'autres messages. Cette notion de sécurité forte n'est pas une fantaisie des cryptographes, mais provient de la nécessité de tenir compte d'environnements peu contrôlés, comme celui d'un serveur WEB répondant aux requêtes.

Nous avons donc cherché à étudier comment transformer, de façon générique, un schéma minimalement sûr en schéma sûr au sens le plus fort. Nous avons proposé de telles transformations [59, 53], dont une en collaboration avec un chercheur japonais Tatsuaki Okamoto. Nous avons ensuite appliqué cette transformation à deux schémas de chiffrement à clé publique basés respectivement sur deux problèmes difficiles à résoudre de théorie des nombres (le problème des hauts-résidus et le problème Diffie-Hellman). Ceci nous a permis d'obtenir – dans le modèle de l'oracle aléatoire – la sécurité de schémas qui ne sont pas fondamentalement plus coûteux en ressources de calcul que le RSA.

D'une certaine façon, nos travaux ont constitué un prolongement de ceux de Bellare et Rogaway qui avaient introduit en 1994 la première conversion générique, appelée OAEP. On a longtemps cru qu'OAEP conduisait à un schéma de chiffrement sûr au sens le plus fort à partir de toute permutation à trappe (outil de théorie de la complexité modélisant le RSA). Pour cette raison, OAEP est devenu une norme internationale adoptée notamment dans SET (Secure Electronic Transactions), protocole mis au point par Mastercard

et Visa pour sécuriser les transactions par cartes bancaires transitant par l'Internet. Cependant, récemment, une faille a été trouvée dans la preuve de sécurité. En collaboration avec des chercheurs de NTT, nous avons alors immédiatement tenté de réparer la preuve, au moins pour son application à RSA. A la surprise de beaucoup, nous y sommes très rapidement parvenus, sauvant ainsi toutes les applications pratiques [87].

3 Authentification mutuelle et échange de clés

La mise en accord de clés de session authentifiées est une notion cruciale pour tous les réseaux informatiques. En effet, tous les protocoles de sécurité de l'Internet et notamment SSL (Secure Socket Layer) qui permet d'ouvrir des connexions sécurisées ne mettent en œuvre la cryptographie à clé publique que pour que les deux parties concernées (client et serveur) s'authentifient et mettent une clé de session en commun (qu'eux seuls connaissent). Ils peuvent alors ensuite utiliser ce secret commun pour passer aux mécanismes de chiffrement conventionnels bien plus rapides. Ce paradigme admet cependant de très nombreuses spécificités selon les applications, et selon ce que les deux parties connaissent ou sont en mesure de calculer.

En collaboration avec Mihir Bellare et Phil Rogaway, nous avons formalisé les notions de sécurité souhaitées pour des schémas généraux de mise en accord de clé de session authentifiée [20]. Puis nous avons élaboré et prouvé un protocole permettant à un client de s'authentifier auprès d'un serveur dans les conditions suivantes : le client et le serveur partagent un mot de passe π secret (mémorisable, donc confiné dans un petit dictionnaire susceptible d'être exploré par une recherche exhaustive) ; le client et le serveur prouvent mutuellement leur connaissance de π, un client et/ou un serveur malhonnêtes ne peuvent rien apprendre sur π, si ce n'est supprimer un élément par interaction, dans la liste des mots de passe possibles. De plus, à la fin de la procédure d'authentification, le client et le serveur possèdent une clé secrète commune, permettant un dialogue sécurisé. Nous avons également réclamé la propriété de "forward secrecy" qui exige que la confidentialité des précédentes communications est maintenue même après la compromission du mot de passe. Notre étude de sécurité a notamment permis de fournir une preuve de sécurité pour un schéma classiquement connu, mais dont la sécurité n'était qu'heuristique. Encore une fois, la nécessité de garantir un niveau de sécurité très élevé, en particulier la forward secrecy, n'est pas un caprice de théoricien mais une nécessité reconnue aujourd'hui, par exemple pour les protocoles normalisés par l'IETF. En revanche, c'est bien à notre avis la thérie qui a constitué l'essentiel de notre démarche : la partie la plus importante de notre travail a précisément été la formalisation des notions de sécurité.

Plus récemment, avec Markus Jakobsson, nous avons travaillé sur un

nouveau schéma de mise en accord de clé de session authentifiée qui exige une quantité minimale de calculs de la part d'un des participants (le client). La méthode passe par le précalcul de certaines données et s'inspire de mécanismes décrits plus haut dans le cadre des signatures au vol [35].

Enfin, nous avons également étudié, avec des collègues Belges, des schémas de mise en accord de clé de session au sein d'un groupe [99]. Il convenait, dans un premier temps, de formaliser les notions de sécurité souhaitables, puis ensuite de proposer et prouver des protocoles, tout en maintenant un niveau élevé d'efficacité. En effet, même si plusieurs schémas avaient déjà été proposés dans la littérature, aucun n'admettait de preuve de sécurité, pour la simple raison qu'aucune spécification des besoins, en terme de sécurité, n'avait jamais été établie. Ce travail a débouché sur un article proposant un modèle de sécurité et un protocole prouvé sûr dans ce modèle ; il a été soumis à la conférence Crypto'2001, et sera probablement par d'autres articles, affinant et développant ce modèle de sécurité.

4 Nouveaux problèmes difficiles

Au travers des différents protocoles présentés dans les paragraphes précédents, le groupe a été amené à proposer de nouveaux problèmes difficiles au sens de la théorie de la complexité, comme base de la cryptographie. C'est ainsi que nous avons introduit le problème de la haute-résiduosité et le problème du RSA-Dépendant. Le premier généralise le problème de la résiduosité quadratique lié à la difficulté de distinguer les carrés modulo un entier n de factorisation inconnu. Le second formalise la difficulté de reconnaître des couples de chiffrés RSA dont les clairs sont liés simplement (par exemple consécutifs). Plus récemment, une des conversions génériques mentionnées dans le paragraphe précédent nous a amené à considérer une nouvelle famille de problèmes, que nous avons dénommés les "Gap Problems" [54]. Il s'agit de résoudre un problème calculatoire étant donné l'accès à un oracle décisionnel. Typiquement, peut-on calculer la fonction de Diffie-Hellman (qui associe à g, g^x et g^y la valeur g^{xy}) en ayant accès à un programme qui détermine seulement si le résultat est correct. Cette famille est à la fois très générale et très utile : elle nous a en effet également permis de prouver la sécurité d'une signature indéniable, proposée en 1989. Cette dernière n'avait jamais pu être conduite, car le problème sous-jacent n'avait pas été identifié.

Depuis, plusieurs autres analyses de sécurité ont fait intervenir cette nouvelle classe de problèmes. Un récent travail sur la signature en blanc de Chaum nous a conduit ainsi à isoler une nouvelle variante du problème RSA [19]. Les nouveaux problèmes sont à leur tour la base de nouvelles investigations : La sécurité de tout protocole cryptographique repose sur la difficulté d'un problème algorithmique donné et la mise en évidence de nouveaux problèmes ouvre la voie à la conception de nouveaux types de

protocoles.

5 Conception de nouveaux algorithmes à clé publique

C'est un défi majeur de la recherche en cryptologie. En un peu plus de vingt ans, la liste des algorithmes à clé publique ne s'est enrichie que d'une dizaine d'exemples venant s'ajouter au RSA. En collaboration avec David Naccache, nous avons imaginé deux cryptosystèmes différents de RSA [41, 42]. Le premier est une généralisation multiplicative du célébre sac-à-dos inventé en 1978 et cassé par Adi Shamir en 1982. En nous fondant sur notre expertise de la cryptanalyse (voir paragraphe suivant), nous pensons que la multiplicativité permet bien d'échapper aux attaques analogues à celle de Shamir. L'autre cryptosystème est basé sur le problème de la haute-résiduosité introduit plus haut. Ce système a de plus des propriétés algébriques d'homomorphisme qui ouvrent la voie à de nombreuses applications, notamment pour le vote électronique. De fait, c'est le premier exemple d'un cryptosystème "homomorphe" ayant une bande passante importante. Noter travail a inspiré des recherches présentées ultérieurement, par Okamoto et Uchiyama d'une part, par Paillier d'autre part. La forme du système de Paillier, plus proche du RSA, est sans doute plus élégante mais nous avons clairement ouvert la voie.

6 Cryptanalyse des systèmes à clé publique

Le GRECC a une très longue expertise, théorique et pratique, dans ce domaine, fondée notamment sur sa maîtrise de l'algorithme LLL de réduction des réseaux, attestée par plusieurs thèses et de nombreuses cryptanalyses "spectaculaires".

En systématisant l'usage du réseau *orthogonal* [108, 13] d'un réseau de dimension incomplète, le groupe a pu cryptanalyser [50] un nouveau cryptosystème proposé par Ajtai et Dwork et présenté par les Laboratoires de recherche IBM comme une découverte majeure. Le système d'Ajtai-Dwork avait d'ailleurs eu les honneurs de la presse. Il était en effet efficace tout en s'appuyant sur une preuve de sécurité profonde. Nous avons d'une certaine manière inversé le paradigme de la sécurité prouvée en montrant que, à moins d'utiliser des paramètres enlevant toute crédibilité au système, on se trouvait face à un problème algorithmique plus accessible que ne l'imaginaient les auteurs. La même méthode a permis d'attaquer [51] un mécanisme de calcul de signatures RSA faisant intervenir un serveur non protégé et de résoudre le problème des sous-ensembles cachés [52], dont la difficulté supposée était à la base d'un système proposé à Eurocrypt '98 pour accélérer la génération de signatures DSA.

Le groupe a également attaqué avec succès plusieurs cryptosystèmes [48, 49, 45] proposés récemment comme alternatives au système RSA, en particulier celui de Goldreich-Goldwasser-Halevi [45], proposé par des chercheurs du MIT et fondé sur la difficulté de certains problèmes liés aux réseaux à coordonnées entières. Le groupe s'est aussi intéressé à des techniques génériques pour attaquer des primitives cryptographiques : réduction probabiliste à des problèmes de réduction de réseaux pour résoudre des problèmes liés à la théorie des codes correcteurs d'erreur ou à la théorie des nombres [21] ; extensions de la méthode de Coppersmith à base de réduction de réseaux pour trouver des petites racines d'équations polynomiales afin d'attaquer des variantes de RSA [26]. Le groupe a mis en avant la vulnérabilité de la signature DSA (et de ses variantes) lorsque l'on connaît un peu d'information sur les paramètres secrets utilisés [46, 106, 27, 107]. Le groupe a montré de façon simple pourquoi l'utilisation naïve de RSA ou ElGamal pour chiffrer des clefs de session symétriques était dangereuse [22], soulignant ainsi l'importance des schémas de type OAEP pour renforcer les notions de sécurité.

On mentionnera pour terminer un travail de cryptanalyse réalisé avec Don Coppersmith [6] qui a permis de "casser" un schéma de signature numérique proposé par Adi Shamir et reposant sur la théorie des permutations birationnelles.

7 Cryptanalyse des systèmes symétriques

Paradoxalement, le domaine de la cryptographie conventionnelle est resté pendant longtemps très pauvre en résultats de cryptanalyse de nature conceptuelle. En 1991, la situation a changé avec l'invention par Biham et Shamir, de la méthode d'attaque "différentielle", suivie en 1996 de la méthode "linéaire" de Matsui. La première méthode étudie des hypothèses de propagation des différences (xor bit à bit) qui ont une probabilité petite mais significative, tandis que la seconde s'intéresse aux relations linéaires sur les bits (de clair, de chiffré ou de clé) qui ont un biais statistique petit mais significatif.

Le groupe a généralisé ces attaques statistiques, ce qui a permis d'améliorer, par un test du χ^2, la meilleure attaque connue contre le standard de chiffrement DES. Il a également proposé dans [63] un critère général de résistance contre l'attaque de Davies et Murphy, attaque contre laquelle DES semble "miraculeusement" protégé, mais qui peut affecter l'importante fraction des cryptosystèmes symétriques qui utilisent une structure fondée sur un schéma de Feistel. Il a aussi montré dans [32] que les attaques par différentielles tronquées sont compliquées à mettre en œuvre et que certaines attaques publiées sont erronées.

Contre l'algorithme Blowfish de Bruce Schneier, on a montré qu'une classe significative de clefs secrètes était particulièrement faible, car elles

conduisaient à une attaque effective. Enfin, le groupe a exercé une activité importante dans l'étude de la sécurité des candidats au processus de standardisation AES, puis du projet européen NESSIE (voir [31, 80, 79, 88, 90, 112]).

Dans le domaine des systèmes de chiffrement série (stream-ciphers), le groupe a présenté dans [64] une originale cryptanalyse de l'algorithme A5/1 du GSM. Cette attaque se fonde sur un compromis logiciel/matériel : un programme structure des données extrêmement simples qui sont ensuite traîtées par un FPGA. Le découpage des tâches entre une station de travail conventionnelle et une carte d'extension contenant quelques FPGA permet d'effectuer une cryptanalyse plusieurs dizaines de fois plus vite qu'avec chacun de ces deux matériels considérés séparément. Enfin, en utilisant ces mêmes matériels à base de FPGA, le groupe a conçu une implantation effective de DES dans le cadre d'un système de recherche exhaustive de clés.

8 Conception et implantation d'algorithmes symétriques

Constatant le passage d'un stade empirique à un stade heuristique, où les algorithmes sont conçus pour résister aux attaques différentielle et linéaire, le groupe a acquis une expertise dans la conception d'algorithmes conventionnels (à clé secrète). Il a ainsi mis au point l'algorithme de chiffrement CS-Cipher [73, 76] qui réalise un bon compromis entre efficacité et sécurité heuristique. Il a également, dans le cadre d'un contrat avec l'ETSI, défini une norme qui sera utilisé dans les futurs téléphones GSM (extension CTS).

En s'inspirant du travail mené dans le secteur de la clef publique, le groupe a tenté de dépasser la sécurité heuristique pour aller vers une sécurité formelle. En utilisant la notion de hachage universel de Carter et Wegman, on a pu bâtir une "théorie de la décorrélation". Cette nouvelle théorie décrite dans [15, 92, 75, 86], offre des outils de calcul symbolique qui permettent de démontrer, dans un modèle abstrait, des résultats de sécurité, notamment face aux attaques différentielles. C'est avec ces principes qu'a été développé le candidat DFC[31, 70, 79, 33] au processus de standardisation AES ; DFC a également été pensé afin d'être implantable efficacement sur les ordinateurs personnels d'aujourd'hui et de demain, en profitant des opérations natives et optimisées des processeurs centraux.

Par ailleurs, en liaison avec l'équipe de Jean Vuillemin, l'équipe a acquis une expérience des architectures matérielles, qui lui a permis d'implanter efficacement les algorithmes ci-dessus sur FPGA ; ce type de puce reconfigurable est déjà extrêmement répandu dans les systèmes embarqués récents, et devient le standard de fait des équipements de chiffrement à haut débit.

Le groupe a également étudié la méthode d'implantation logicielle dite du "code orthogonal", technique redécouverte en 1997 par Eli Biham sous le nom de "bitslice" ; cette méthode consiste principalement en l'émulation

de plusieurs implantations matérielles en parallèle, en répartissant les bits de données à traiter sur tous les registres du processeur. Afin de faciliter la conception et la mise au point de programmes utilisant cette technique, l'équipe a programmé et mis à disposition du public un compilateur[118] émettant le code C réalisant, suivant la méthode orthogonale, un cryptosystème qui lui est fourni sous la forme d'une description formelle de haut niveau.

Enfin, le groupe a travaillé sur la conception de nouveaux algorithmes optimisés pour ces implantations matérielles ou logicielles, afin de résoudre les besoins croissants en débit de chiffrement des matériels moderne ; un tel algorithme, ainsi qu'une étude de son utilisation pour le chiffrement transparent d'un disque dur d'ordinateur portable, sont proposés dans [111].

9 Cryptographie "interactive"

Le contexte de la cryptographie traditionnelle, qui met en jeu deux entités seulement n'est plus complètement adapté à la réalité multiforme de l'Internet. Dans de nombreux scénarios, vote électronique, enchères en ligne etc., de nombreux acteurs coopèrent.

Le GRECC a étudié la question de la génération commune d'une clé RSA par deux entités distantes à la suite des travaux de Boneh et Franklin [66]. Il a également proposé la première méthode de génération de clés cryptographiques pour les systèmes fondés sur le logarithme discret, qui ne nécessite pas l'établissement antérieur, entre les participants, d'un canal "privé" [30]. Ceci a l'avantage d'éviter la mise en accord de clé entre chaque paire d'utilisateurs et donc d'améliorer la génération partagée de la clé. Par ailleurs, il a pu montrer [29] comment construire une architecture de déchiffrement répartie pour le système de chiffrement homomorphique de Paillier. Durant ce travail, nous avons défini un modèle de sécurité pour les algorithmes de déchiffrement partagé à seuil.

En utilisant précisément le système de Paillier il a été possible de concevoir un système global de vote électronique qui autorise une bien meilleure sécurité que ceux proposés antérieurement [97]. De même a-t-on pu appliquer le même schéma pour proposer un protocole d'enchères anonymes sur le Web [17]. Ce protocole permet la détermination du vainqueur sans que les enchères des autres participants ne soient révélées. Le prix payé peut être, au choix, l'enchère la plus élevée ou la seconde, plus proche du résultat d'enchéres traditionnelles à l'anglaise.

A la suite du travail sur le vote électronique, il est apparu que le partage de l'autorité de vote est un élément essentiel d'un schéma de vote. Le groupe a proposé une solution élégante au problème de génération d'une clé RSA tout en permettant au protocole de signature ou de déchiffrement partagé de s'effectuer de manière robuste [103]. Il est enfin possible de préserver secrète

une clé RSA partagée, de sa création à son utilisation. C'est là un résultat qui devrait avoir des applications.

Enfin, le GRECC s'est récemment penché sur les problèmes cryptographiques relevant de l'anonymat. Il a proposé le premier schéma de signature collective permettant d'exclure des membres malhonnêtes d'un groupe sans être obligé de modifier les paramètres publics régissant ce groupe [23]. Ce travail s'appuyait sur les schémas de signature de groupe proposés en 1997 par Camenish et Stadler. Depuis, nous avons formalisé cette méthode pour la rendre applicable à d'autres schémas, tout en la plaçant dans un cadre théorique plus général [100].

10 Perspectives

La cryptologie moderne a à peine plus de vingt ans. Dans sa courte histoire, elle a eu la chance de connaître deux avancées majeures :

- l'invention en 1976 de la cryptographie à clé publique et des signatures numériques
- la découverte en 1986 du concept de "zero-knowledge"

Ces deux découvertes ont été chacune le moteur de dix années de recherche intense. Aujourd'hui, l'heure est à la consolidation, pour deux raisons au moins

1. Les outils conceptuels permettant de mener des analyses conceptuelles de sécurité sont enfin au point. A noter qu'il s'agit d'un état de fait extrêmement récent : la façon absolument correcte d'utiliser RSA est issue d'un long cheminement qui vient de s'achever avec les travaux sur OAEP auxquels le groupe a participé.
2. Compte tenu des besoins de sécurité de l'Internet et du commerce électronique, il existe un fort appel de solutions crypto épurées et/ou normalisées.

Le groupe compte donc poursuivre son travail de *validation*, avec les lignes de force suivantes :

- Validation par preuve de sécurité : le champ d'action est vaste. de nombreux protocoles d'échange de clé de session, notamment, même en voie de normalisation, reposent actuellement sur une simple analyse heuristique.
- Validation par cryptanalyse : certains schémas cryptographiques, y compris parmi ceux mis sur le marché pour répondre à des demandes spécifiques, pourraient présenter des failles. C'est le cas – à notre avis – du système NTRU. Notre avance en cryptanalyse laisse entrevoir des résultats.
- Validation par distribution : ce sera, pensons nous, une exigence prochaine pour certains systèmes déployés dans les infrastructures de clés

publiques (PKI). Une application hautement sécurisée ne saurait laisser une clé secrète indivise. Là encore, notre expertise de la cryptologie interactive devrait nous permettre de proposer des solutions originales pour le partage de clés cryptographqiues dans nombre de situations.

Enfin, dans la mesure du possible, nous comptons ouvrir de nouveaux fronts, en utilisant en particulier l'interface avec les autres équipes du laboratoire. Ainsi, l'analyse *logique* des protocoles cryptographique (dans l'esprit des travaux de M. Abadi à Stanford) est un sujet qui s'inscrit naturellement dans cette perspective.

Éléments d'évaluation

1 Collaborations

- Projet Européen
  - *New European Schemes for Signature, Integrity and Encryption.*
    (NESSIE : `http://www.cryptonessie.org/`).
    Début : janvier 2000. Fin : décembre 2002.
- Contrats avec le CELAR
  - *Étude de systèmes de chiffrement symétrique par blocs.*
    Début : mars 2000. Fin : octobre 2001.
  - *Veille technologique.*
- Contrat OPPIDUM/Confiance avec le Ministère de l'Economie des Finances et de l'Industrie
  Début : juin 1999. Fin : juin 2001.
- Contrat avec le CNRS sur les Stratégies de Recouvrement sur les couches basses de l'Internet
  Début : 20 mai 1998. Fin : 20 mai 2000.
- Contrat avec la DCSSI sur les Mécanismes cryptographiques distribués
  Début : 16 septembre 1999. Fin : 16 octobre 2000.
- Contrat avec France Telecom R&D sur les Mécanismes d'Anonymat pour la Signature et le Chiffrement
  Début : 21 octobre 1999. Fin : 21 octobre 2001.
- Contrat avec l'ETSI (European Telecommunication Standards Institute) : Développement d'un algorithme de chiffrement pour le projet CTS (Cordless Telephone System)
  Début : 15 février 1999. Fin : 31 décembre 1999.
- Échanges avec Israël (convention franco-israélienne Arc-en-ciel)

2 Missions, conférences et séminaires

- O. Baudron : conférences à Helsinki, Finlande (*Eurocrypt'98*, mai 1998), Le Croisic, France (*27ème École de Printemps d'Informatique Théorique*, June 1999), Prague, République Tchèque (*Eurocrypt'99*, mai 1999), Bruges, Belgique (*Eurocrypt 2000*, mai 2000), Genève,

Suisse (*ICALP 2000*, juillet 2000), Santa Barbara, USA (*Crypto 2000*, août 2000).

- E. Bresson : conférences à Bruges, Belgique (*Eurocrypt'2000*, mai 2000), Kyoto, Japon (*Asiacrypt'2000*, décembre 2000), Cheju, Corée (*PKC'2001*, février 2001).
- P.A. Fouque : conférences à Santa Barbara, USA (*Crypto'99*, août 1999 – *Crypto'2000*, août 2000), Anguilla, BWI (*Financial Crypto '00*, février 2000), Prague, République Tchèque (*Eurocrypt'99*, mai 1999), Bruges, Belgique (*Eurocrypt'2000*, mai 2000), Leuven, Belgique (novembre 2000), Cheju, Corée du Sud (*PKC'2001*, février 2001).
- L. Granboulan : conférences à Sophia-Antipolis, France (*Journées de géometrie algorithmique*, mai 1998), Santa Barbara, USA (*Crypto'98*, août 1998 – *Crypto'99*, août 1999), New York, USA (*FSE'2000* et *AES3*, avril 2000), Bruges, Belgique (*Eurocrypt'2000*, mai 2000), Leuven, Belgique (*First NESSIE Workshop*, novembre 2000) ; réunions de travail du projet NESSIE à Leuven, Belgique (avril 1999), Eilat, Israël (janvier 2000), Leuven, Belgique (février 2000), New York, USA (avril 2000), Bruges, Belgique (mai 2000), Leuven, Belgique (février 2001).
- G. Martinet : conférence à Leuven, Belgique (*First NESSIE Workshop*, novembre 2000) ; réunions de travail du projet NESSIE à Leuven, Belgique (novembre 2000), Leuven, Belgique (février 2001).
- P. Nguyen : conférences à Santa Barbara, USA (*Crypto '97*, août 1997 – *Crypto '98*, août 1998 – *Crypto '99*, août 1999 – *Crypto '2000*, août 2000), Portland, USA (*ANTS-III*, juin 1998), Beijing, Chine (*Asiacrypt '98*, octobre 1998), Kamakura, Japon (*PKC '99*, mars 1999) Luminy, France (*CIRM Workshop*, septembre 1999) Singapour (*CCNT '1999*, novembre 1999), Bruges, Belgique (*Eurocrypt '2000*, mai 2000), Berkeley, USA (*MSRI workshop*, octobre 2000), Kyoto, Japon (*Asiacrypt '2000*, décembre 2000), Séoul, Corée (*KIAS Cryptography Initiative*, décembre 2000), Oberwolfach, Allemagne (*Workshop on finite fields*, janvier 2001) ; séjours pour collaboration à IBM (USA, Août 1999 et Mai 2000), Lucent Bell Labs (USA, Août 1999 et Juillet–Septembre 2000), Microsoft Research (USA, Février 2000), Stanford Univ. (USA, Mars 2000), Univ. of Macquarie (Australie, Novembre 2000), Univ. of Bristol (Grande-Bretagne, Février 2001).
- D. Pointcheval : conférences à Zurich, Suisse (*ACM Conference on Computer and Communications Security*, avril 1997), Santa Barbara, USA (*Crypto '97*, août 1997 – *Crypto '98*, août 1998 – *Crypto '2000*, août 2000), Dagstuhl, Allemagne (*WorkShop de Cryptographie*, septembre 1997), Les Tourelles, France (*Rencontre AMI/C2*, février 1998), Monte Verita, Suisse (*WorkShop de Cryptographie*, mars 1998), Espoo, Finlande (*Eurocrypt '98*, juin 1998), Prague, République Thèque (*Eurocrypt '99*, mai 1999), Batz-sur-Mer, France (*École de Printemps d'Informatique Théorique - Cryptographie et Codage*, juin 1999), Luminy,

France (*Colloque de Cryptographie*, septembre 1999), Singapour (*Asiacrypt '99*, novembre 1999), Melbourne, Australie (*PKC '2000*, janvier 2000), Bruges, Belgique (*Eurocrypt '2000*, mai 2000), Grand Cayman, BWI (*Financial Cryptography '01*, février 2001).
Conférencier invité à Pohang, Corée du Sud (*Com2MaC Workshop : Present and Future*, février 2000), Pohang, Corée du Sud (*Com2MaC Workshop : Cryptography*, juin 2000), Tokyo, Japon (*The 4th Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography*, novembre 2000).
Séminaires à Univ. Lille I (*Séminaires du CALC et du LIFL*, avril 1997), Univ. de Californie à San Diego, USA (octobre 1997), Univ. de Communication et d'Information, Taejon, Corée du Sud (juin 2000), EPFL, Lausanne, Suisse (*Séminaire "Summer Research Institute"*, juillet 2000), Lucent Technologies, New Jersey, USA (août 2000), Tokyo, Japon (novembre 2000), ENSTA, Paris, France (*Séminaire Cryptographie, Codage et Algorithmique*, décembre 2000), Univ. Caen (*Séminaire du GREYC*, janvier 2001).
Séjours pour collaboration à Université de Californie à San Diego, USA (octobre-décembre 1997), Lucent Technologies, New Jersey, USA (août 2000), NTT, Tokyo, Japon (novembre 2000).

– T. Pornin : conférences à Santa Barbara, USA (*Crypto'97*, août 1997 – *Crypto'2000*, août 2000), Paris, France (*FSE'98*, mars 1998), Beijing, Chine (*Asiacrypt'98*, octobre 1998), Rome, Italie (*FSE'99*, mars 1999), Prague, République Tchèque (*Eurocrypt'99*, mai 1999), New York, USA (*FSE'2000*, avril 2000), Bruges, Belgique (*Eurocrypt'2000*, mai 2000), Worcester, USA (*CHES'2000*, août 2000).
– G. Poupard : conférences à Les Tourelles, France (*Rencontre AMI/C2*, février 1998), Helsinki, Finlande (*Eurocrypt'98*, mai 1998), Santa Barbara, USA (*Crypto'98*, août 1998 – *Crypto'99*, août 1999), Prague, République Tchèque (*Eurocrypt'99*, mai 1999), Marseilles, France (*Trusting Electronic Trade '99*, Juin 1999), Luminy, France (*CIRM Workshop*, septembre 1999) Singapour (*ACM-CCS '1999*, novembre 1999), Anguilla, BWI (*Financial Crypto '00*, février 2000), Bruges, Belgique (*Eurocrypt 2000*, mai 2000). Séminaires à Weizmann Institue, Rehovot, Israël (Septembre 1999), ENSTA, Paris, France (*Séminaire Cryptographie, Codage et Algorithmique*, mai 2000).
– J. Stern : conférences à Zurich, Suisse (*ACM Conference on Computer and Communications Security*, avril 1997), Anguilla, BWI (*Financial Cryptography '97*, février 1997). Konstanz, Allemagne (*Eurocrypt'97*, mai 1997), Santa Barbara, USA (*Crypto '97*, août 1997 – *Crypto '98*, août 1998 – *Crypto '99*, août 1999) – *Crypto '2000*, août 2000), Dagstuhl, Allemagne (*WorkShop de Cryptographie*, septembre 1997), Paris, France (*FSE'98*, mars 1998), Monte Verita, Suisse (*WorkShop de Cryptographie*, mars 1998), Espoo, Finlande (*Eurocrypt '98*, juin 1998), Bei-

jing, Chine (*Asiacrypt '98*, octobre 1998), Rome, Italie (*FSE'99*, mars 1999), Prague, République Thèque (*Eurocrypt '99*, mai 1999), Worcester, USA (*CHES'1999*, août 1999), Luminy, France (*Colloque de Cryptographie*, septembre 1999), Singapour (*CCNT '1999*, novembre 1999), Singapour (*Asiacrypt '99*, novembre 1999), Anguilla, BWI (*Financial Crypto '00*, février 2000), Bruges, Belgique (*Eurocrypt '2000*, mai 2000), Worcester, USA (*CHES'2000*, août 2000), Kyoto, Japon (*Asiacrypt '2000*, décembre 2000), Cheju, Corée du Sud (*PKC'2001*, février 2001), Grand Cayman, BWI (*Financial Cryptography '01*, février 2001) ; réunions de travail du projet NESSIE à Leuven, Belgique (avril 1999), Eilat, Israël (janvier 2000).
Conférencier invité à Spitzberg, Norvège (*colloque IEEE*, juillet 1997), Yokohama, Japon (*PKC'98*, novembre 1998), Kruger Park, Afrique du Sud (*colloque IEEE*, juin 1999), Amalfi, Italie (*Second workshop on security in communications networks*, septembre 1999), Waterloo, Canada (*Workshop on elliptic curve cryptography*, novembre 1999), Leyden, Pays Bas, (*ANTS IV*, juillet 2000).
Séjour pour collaboration à Lucent Technologies, New Jersey, USA (mars 2000).

3 Accueil de chercheurs

- **Professeurs et directeurs de recherche invités**
  Eli Biham (Technion), octobre 1997 (professeur invité ENS).
  Avi Rubin (AT&T Labs - Research), mai-juin 1999 (professeur invité ENS).
  Dan Boneh (Université de Stanford), septembre 1999 (professeur invité ENS).
  Birgit Pfitzman (Université de Sarrebruck), février-mars 2001 (professeur invité ENS).

4 Diffusion de la connaissance

- Organisation à Luminy d'un workshop de Cryptographie (septembre 1999)
- Organisation à l'ENS les 11 et 12 juin 1999 du workshop « Automatic text analysis and browsing of big databases ».
  12 exposés et 58 participants.
  `http://www.apim.ens.fr/text.html`
- Organisation à l'ENS les 22 et 23 octobre 1999 du workshop « Watermarking, copyright enforcement ».
  9 exposés et 46 participants.
  `http://www.apim.ens.fr/watermark.html`

– Séminaire « Complexité et Cryptographie ».
Une quinzaine d'exposés par an.
`http://www.di.ens.fr/~wwwgrecc/Seminaire/`
– J. Stern : Conférence à l'Université de tous les savoirs, septembre 2000.

5 Réalisation et diffusion de logiciels, brevets

– David Pointcheval et Serge Vaudenay. *Information Technology - Security Techniques - Digital Signatures with Appendix - Part 3 : Certificate-Based Mechanisms.ISO/IEC 14888-3*, 20 décembre 1998). Incluse la Signature Pointcheval-Vaudenay [89].
– David Arditi, Henri Gilbert, Jacques Stern, et David Pointcheval. *Procédé d'Identification à Clé Publique*. Brevet en France 97-05831, 1997.
– David Arditi, Henri Gilbert, Jacques Stern, et David Pointcheval. *Procédé d'Identification à Clé Publique Utilisant Deux Fonctions de Hachage*. Brevet en France 97-05830 - Brevet en Europe 98401120.5-2209, 1997.

6 Participations à l'évaluation de la recherche

– O. Baudron :
évaluateur pour les conférences Eurocrypt 2000, Crypto 2000, ICALP 2000 et FC 2001.

– L. Granboulan :
évaluateur pour les conférences Asiacrypt 2000, Eurocrypt 2000, Crypto 2000, PKC (1998, 2000 et 2001), SAC 1999, Esorics 2000, ICALP 2000 et pour la revue *Information Processing Letters*.

– P. Nguyen :
membre du comité de programme d'INDOCRYPT 2000 et CALC 2001.

évaluateur pour les revues *Journal of Cryptology*, *IEEE Trans. on Inform. Theory* et *Information Processing Letters*.

évaluateur pour les conférences Eurocrypt (1998 et 2000), PKC (1998, 1999 et 2001), Crypto (1999 et 2000), Asiacrypt (2000), SAC (1998).

– D. Pointcheval :
membre du comité de programme d'Eurocrypt 2000 et ICICS 2001.

évaluateur pour les revues *Journal of Cryptology*, *IEEE Trans. on Inform. Theory*, *IEEE Trans. on Computers*, *Designs, Codes and Cryptography* et *European Transactions on Telecommunications*.

évaluateur pour les conférences Eurocrypt (1998, 1999, 2000 et 2001), PKC (1998, 1999, 2000 et 2001), Crypto (1999 et 2000), Asiacrypt (1999, et 2000), ESORICS (2000), Financial Cryptography (1999 et 2001), STACS (1999 et 2000) et ICALP (2000).

– G. Poupard :

membre du comité de programme d'Eurocrypt 2001.

évaluateur pour les conférences Eurocrypt (1998, 2000 et 2001) et Crypto (1999 et 2000).

– J. Stern :

membre du comité de programme de : ACM Conference on Computer and Communications Security 1997, PKC'98, Financial Cryptography 99, Asiacrypt'99, Eurocrypt'99 Crypto'2000, Asiacrypt'2000, Indocrypt'2000, RSA Conference 2001, PKC'01, Financial Cryptography 01, IFIP-SEC'01, CHES'01

président du Comité de programme, d'Eurocrypt'99

membre du Comité éditorial du *Journal of Cryptology* et de la revue *Transactions on Information and System Security.*

7 Encadrement doctoral

Direction de thèses

– J. Stern

L. Granboulan, *Calcul d'objets géométriques à l'aide de méthodes algébriques et numériques : Dessins d'enfants*[83], Université Paris VII, soutenue en décembre 1997.

P. Q. Nguyen, *La Géométrie des Nombres en Cryptologie*[84], Université Paris VII, soutenue en novembre 1999.

G. Poupard, *Authentification d'entités, de messages et de clés cryptographique : théorie et pratique*[85], École Polytechnique, soutenue en 2000.

S. Vaudenay, *Vers Une Théorie du Chiffrement Symétrique*[86], Habilitation Université Paris VII, soutenue en janvier 1999.

J. Patarin, *La cryptographie multivariable* Habilitation Université Paris VII, soutenue en novembre 2000,

A. Joux, *Méthodes algorithmiques pour la cryptographie* Habilitation Université Paris VII, soutenue en décembre 2000,

J.-S. Coron, soutenance prévue en mai 2001,

T. Pornin, soutenance prévue en septembre 2001,

O. Baudron, soutenance prévue en septembre 2001,

P.-A. Fouque, soutenance prévue en septembre 2001,

Participation à d'autres jurys de thèses
- D. Pointcheval : 2 jurys,
- J. Stern : 11 jurys.

Direction de DEA
- J. Stern : 3 directions

8 Enseignement

Premier et deuxième cycle
- O. Baudron
  Travaux dirigés de programmation à Paris 6.
- E. Bresson
  Travaux dirigés d'algorithmique (programmation en C) à l'ENSTA.
- L. Granboulan
  Travaux dirigés d'algorithmique et de programmation au MMFAI.
  Travaux dirigés de tronc commun d'informatique à l'École Polytechnique.
  Travaux dirigés de programmation système et réseau au MMFAI.
  Organisation des enseignements interdisciplinaires des magistères de l'ENS, thèmes « Les Formes » puis « Le Temps ».
- P. Nguyen
  Travaux dirigés de programmation à Paris 7.
- D. Pointcheval
  Travaux dirigés d'algorithmique en Licence, à l'Université de Caen.
  Travaux dirigés d'algorithmique et de programmation en C à l'Ecole Nationale Supérieure de Techniques Avancées.
  Travaux dirigés d'algorithmique et de programmation en Java à l'Ecole Polytechnique.
  Travaux dirigés de programmation en Java à l'Ecole Nationale Supérieure de Techniques Avancées.
  Cours de programmation en C à l'Ecole Nationale Supérieure de Techniques Avancées.
  Cours de Cryptographie à l'Ecole Nationale des Ponts et Chaussées.
  Cours de Cryptographie à l'Ecole Supérieure d'Informatique-Électronique-Automatique.
  Cours de Théorie des Nombres à l'Ecole Nationale des Ponts et Chaussées.
- T. Pornin
  Travaux dirigés de programmation Pascal à Paris 7.
  Travaux dirigés d'algorithmique (et programmation en C) à Paris 7.
  Travaux dirigés sur les interfaces graphiques à Paris 7.

- G. Poupard
  Cours d'Algorithmique à l'Ecole Nationale Supérieure de Techniques Avancées.
  Travaux dirigés d'algorithmique et de programmation en Java à l'Ecole Polytechnique.
  Travaux dirigés d'algorithmique à l'Ecole Nationale Supérieure de Techniques Avancées.
  Travaux dirigés de programmation en C à l'Ecole Nationale Supérieure de Techniques Avancées.
- J. Stern
  Magistère de mathématique et informatique de l'ENS : cours d'algorithmique et programmation.

Troisième cycle
- J.Stern
  DEA Algorithmique : cours de cryptographie.

9 Prix et distinctions

Phong Nguyen a reçu un Troisième prix d'Alembert des lycéens en 2000, décerné par la SMF pour la vulgarisation des mathematiques. Il a reçu un prix de thèse 1999 de l'Association Française d'Informatique Théorique et un accessit du prix de thèse 2000 de l'association Specif.

Jacques Stern a été nommé Chevalier de la légion d'honneur en 2000.

Publications

Livres

[1] J. Stern. – *La science du secret.* – Odile Jacob, 1999.

Édition d'actes ou d'ouvrages collectifs

[2] A. Odlyzko, C. P. Schnorr, A. Shamir et J. Stern (éditeurs). – *Cryptography.* – Dagstuhl Seminar Report ; 190, sept. 1997.

[3] J. Stern (éditeur). – *Advances in Cryptology – Proceedings of Eurocrypt '99.* – Springer-Verlag, Berlin, 1999, *Lecture Notes in Computer Science*, vol. 1592.

[4] S. Vaudenay (éditeur). – *Fast Software Encryption, Fifth International Workshop, Paris, France, Proceedings, March 1998.* – Springer-Verlag, Berlin, 1998, *LNCS*, vol. 1372.

Articles dans des revues internationales avec comité de lecture

[5] S. Arora, L. Babai, J. Stern et Z. Sweedyk. – The hardness of approximating problems defined by linear constraints. *J of Comp. Syst. Sci.*, vol. 54, 1997, pp. 317–331.

[6] D. Coppersmith, J. Stern et S. Vaudenay. – Attacks on the birational permutation signature. *Journal of Cryptology*, vol. 10, n° 3, Summer 1997, pp. 207–221.

[7] J. Friedman, A. Joux, Y. Roichman, J. Stern et J.-P. Tillich. – The action of a few random permutations is quickly r-transitive. *Random Structures and Algorithms*, vol. 12, n° 4, 1998, pp. 335–350.

[8] A. Joux et J. Stern. – Lattice reduction : a toolbox for the cryptanalyst. *Journal of Cryptology*, vol. 11, 1998, pp. 161–185.

[9] D. Pointcheval. – Secure Designs for Public-Key Cryptography based on the Discrete Logarithm. *Discrete Applied Mathematics*, 2001. – To appear.

[10] D. Pointcheval et J. Stern. – Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, vol. 13, n° 3, 2000, pp. 361–396.

[11] G. Poupard. – A Realistic Security Analysis of Identification Schemes based on Combinatorial Problems. *European Transactions on Telecommunications*, vol. 8, 1997, pp. 471–480.

Conférences invitées

[12] P. Q. Nguyen. – The two faces of lattices in cryptology. *In : Proc. of Cryptography and Lattices Conference '2001. Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[13] P. Q. Nguyen et J. Stern. – Lattice Reduction in Cryptology : An Update. *In : Algorithmic Number Theory – Proceedings of ANTS-IV. Lecture Notes in Computer Science*, vol. 1838. – Springer-Verlag, Berlin, 2000.

[14] D. Pointcheval. – Number Theory and Public-Key Cryptography. *In : Combinatorial and Computational Mathematics*, éd. par J. H. Kwak, K. H. Kim et F. W. Roush. *Lecture Notes in Pure and Applied Mathematics.* – Marcel Dekker, New York, 2000. To appear.

[15] S. Vaudenay. – Provable security for block ciphers by decorrelation. *In : STACS 98*, éd. par M. Morvan, C. Meinel et D. Krob. *LNCS*, vol. 1373. – Springer-Verlag, Berlin, 1998.

Communications dans des conférences internationales avec comité de lecture

[16] O. Baudron, D. Pointcheval et J. Stern. – Extended Notions of Security for Multicast Public-Key Cryptosystems. *In : 27th International Colloquium on Automata Languages and Programming, ICALP 2000*, éd. par U. Montanari, J. Rolim et E. Welzl. *Lecture Notes in Computer Science*, vol. 1853, pp. 499–511. – Springer-Verlag, Berlin, 2000.

[17] O. Baudron et J. Stern. – Non-Interactive Private Auctions. *In : Proceedings of Financial Cryptography 2001*, éd. par P. Syverson. *Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[18] M. Bellare, A. Desai, D. Pointcheval et P. Rogaway. – Relations Among Notions of Security for Public-Key Encryption Schemes. *In : Advances in Cryptology – Proceedings of Crypto '98*, éd. par H. Krawczyk. *Lecture Notes in Computer Science*, vol. 1462, pp. 26–45. – Springer-Verlag, Berlin, 1998.

[19] M. Bellare, C. Namprempre, D. Pointcheval et M. Semanko. – The Power of RSA Inversion Oracles and the Security of Chaum's RSA Blind Signature Scheme. *In : Proceedings of Financial Cryptography '2001*,

éd. par P. Syverson. *Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[20] M. Bellare, D. Pointcheval et P. Rogaway. – Authenticated Key Exchange Secure Against Dictionary Attacks. *In : Advances in Cryptology – Proceedings of Eurocrypt '2000*, éd. par B. Preneel. *Lecture Notes in Computer Science*, vol. 1807, pp. 139–155. – Springer-Verlag, Berlin, 2000.

[21] D. Bleichenbacher et P. Q. Nguyen. – Noisy Polynomial Interpolation and Noisy Chinese Remaindering. *In : Proc. of the 18th IACR Eurocrypt Conference (Eurocrypt '2000). Lecture Notes in Computer Science*, vol. 1807. – Springer-Verlag, Berlin, 2000.

[22] D. Boneh, A. Joux et P. Q. Nguyen. – Why Textbook ElGamal and RSA Encryption are Insecure. *In : Advances in Cryptology – Proceedings of Asiacrypt '2000. Lecture Notes in Computer Science*, vol. 1976. – Springer-Verlag, Berlin, 2000.

[23] E. Bresson et J. Stern. – Efficient Revocation in Group Signatures. *In : Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001)*, éd. par K. Kim. *LNCS*, vol. 1992, pp. 190–206. – Springer-Verlag, Berlin, 2001. To appear.

[24] E. Brickell, D. Pointcheval, S. Vaudenay et M. Yung. – Design Validations for Discrete Logarithm Based Signature Schemes. *In : Workshop on Practice and Theory in Public-Key Cryptography (PKC '2000)*, éd. par H. Imai et Y. Zheng. *Lecture Notes in Computer Science*, vol. 1751, pp. 276–292. – Springer-Verlag, Berlin, 2000.

[25] C. Coupé, P. Q. Nguyen et J. Stern. – The Effectiveness of Lattice Attacks Against Low-Exponent RSA. *In : Proceedings of PKC '99. Lecture Notes in Computer Science*, vol. 1560. – Springer-Verlag, Berlin, 1999.

[26] G. Durfee et P. Q. Nguyen. – Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99. *In : Advances in Cryptology – Proceedings of Asiacrypt '2000. Lecture Notes in Computer Science*, vol. 1976. – Springer-Verlag, Berlin, 2000.

[27] E. El Mahassni, P. Q. Nguyen et I. E. Shparlinski. – The insecurity of nyberg-rueppel and other dsa-like signature schemes with partially known nonces. *In : Proc. of Cryptography and Lattices Conference '2001. Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[28] P. Fouque, G. Poupard et J. Stern. – Recovering Keys in Open Networks. *In : Proceedings of IEEE Information Theory and Communications Workshop.* – 1999.

[29] P. Fouque, G. Poupard et J. Stern. – Sharing Decryption in the Context of Voting or Lotteries. *In : Financial Cryptography 2000. LNCS.* – Springer-Verlag, Berlin, 2000.

[30] P. Fouque et J. Stern. – One Round Threshold Discrete-Log Key Generation without Private Channels. *In : Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001)*, éd. par K. Kim. *LNCS*, vol. 1992, pp. 190–206. – Springer-Verlag, Berlin, 2001.

[31] H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern et S. Vaudenay. – Decorrelated Fast Cipher : an AES Candidate. *In : First Advanced Encryption Standard (AES) Candidate Conference.* – 1998.

[32] L. Granboulan. – Flaws in differential cryptanalysis of Skipjack. *In : Fast Software Encryption : 8th International Workshop*, éd. par M. Matsui. – Springer-Verlag, Berlin, 2001. à paraître.

[33] L. Granboulan, P. Q. Nguyen, F. Noilhan et S. Vaudenay. – DFCv2. *In : Selected Areas in Cryptography – Proc. of SAC '2000. Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2000.

[34] H. Handschuh et S. Vaudenay. – A universal encryption standard. *In : Selected Areas on Cryptography, Kingston, Ontario, Canada, Proceedings, August 1999*, éd. par H. Heys et C. Adams. *LNCS*, vol. 1758, pp. 1–12. – Springer-Verlag, Berlin, 2000.

[35] M. Jakobsson et D. Pointcheval. – Mutual Authentication for Low-Power Mobile Devices. *In : Proceedings of Financial Cryptography '2001*, éd. par P. Syverson. *Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[36] M. Jakobsson, D. Pointcheval et A. Young. – Secure Mobile Gambling. *In : RSA Cryptographers' Track (RSA '2001)*, éd. par D. Naccache. *Lecture Notes in Computer Science.* – Springer-Verlag, Berlin, 2001.

[37] D. M'Raïhi, D. Naccache, D. Pointcheval et S. Vaudenay. – Computational Alternatives to Random Number Generators. *In : Proceedings of Selected Areas in Cryptography '98*, éd. par S. Tavares et H. Meijer. *Lecture Notes in Computer Science*, vol. 1556. – Springer-Verlag, Berlin, 1999.

[38] D. M'Raïhi, D. Naccache, J. Stern et S. Vaudenay. – xmx : a firmware-oriented block cipher based on modular multiplications. *In : Fast Software Encryption, Fourth International Workshop, Haifa, Israel, Proceedings, January 1997*, éd. par E. Biham. *LNCS*, vol. 1267, pp. 166–171. – Springer-Verlag, Berlin, 1997.

[39] D. M'Raïhi et D. Pointcheval. – Distributed Trustees and Revokability : a Framework for Internet Payment. *In : Proceedings of Financial*

Cryptography '98, éd. par R. Hirschfeld. *Lecture Notes in Computer Science*, vol. 1465, pp. 28–41. – Springer-Verlag, Berlin, 1998.

[40] D. Naccache, D. Pointcheval et C. Tymen. – Monotone Signatures. *In : Proceedings of Financial Cryptography '2001*, éd. par P. Syverson. *Lecture Notes in Computer Science*. – Springer-Verlag, Berlin, 2001.

[41] D. Naccache et J. Stern. – A new public key cryptosystem. *In : Advances in Cryptology – Proceedings of EUROCRYPT '97*, éd. par W. Fumy. *Lecture Notes in Computer Science*, vol. 1233, pp. 27–36. – Springer-Verlag, Berlin, 1997.

[42] D. Naccache et J. Stern. – A new cryptosystem based on higher residues. *In : Proceedings of the 5th ACM Conference on Computer and Communications Security*. pp. 59–66. – ACM press, 1998.

[43] D. Naccache et J. Stern. – Signing on a postcard. *In : Proceedings of FINANCIAL CRYPTOGRAPHY '00. Lecture Notes in Computer Science*. – Springer-Verlag, Berlin, 2000.

[44] P. Q. Nguyen. – A Montgomery-like Square Root for the Number Field Sieve. *In : Algorithmic Number Theory – Proceedings of ANTS-III. Lecture Notes in Computer Science*, vol. 1423. – Springer-Verlag, Berlin, 1998.

[45] P. Q. Nguyen. – Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97. *In : Proc. of the 19th IACR Cryptology Conference (Crypto '99). Lecture Notes in Computer Science*, vol. 1666. – Springer-Verlag, Berlin, 1999.

[46] P. Q. Nguyen. – The Dark Side of the Hidden Number Problem : Lattice Attacks on DSA. *In : Proc. of Workshop on Comp. Number Theory and Cryptography (CCNT'99)*. – Birkhäuser, 2000.

[47] P. Q. Nguyen, I. E. Shparlinski et J. Stern. – Distribution of Modular Sums and Security of Server-Aided Exponentiation. *In : Proc. of Workshop on Comp. Number Theory and Cryptography (CCNT'99)*. – Birkhäuser, 2000.

[48] P. Q. Nguyen et J. Stern. – Merkle-Hellman Revisited : a Cryptanalysis of the Qu-Vanstone Cryptosystem Based on Group Factorizations. *In : Proc. of the 17th IACR Cryptology Conference (Crypto '97). Lecture Notes in Computer Science*, vol. 1294, pp. 198–212. – Springer-Verlag, Berlin, 1997.

[49] P. Q. Nguyen et J. Stern. – Cryptanalysis of a fast public key cryptosystem presented at SAC '97. *In : Selected Areas in Cryptography – Proc. of SAC '98. Lecture Notes in Computer Science*, vol. 1556. – Springer-Verlag, Berlin, 1998.

[50] P. Q. Nguyen et J. Stern. – Cryptanalysis of the Ajtai-Dwork Cryptosystem. *In : Proc. of the 18th IACR Cryptology Conference (Crypto*

'98). Lecture Notes in Computer Science, vol. 1462, pp. 223–242. – Springer-Verlag, Berlin, 1998.

[51] P. Q. Nguyen et J. Stern. – The Béguin-Quisquater Server-Aided RSA Protocol from Crypto '95 is not Secure. *In : Advances in Cryptology – Proceedings of Asiacrypt '98. Lecture Notes in Computer Science*, vol. 1514. – Springer-Verlag, Berlin, 1998.

[52] P. Q. Nguyen et J. Stern. – The Hardness of the Hidden Subset Sum Problem and its Cryptographic Implications. *In : Proc. of the 19th IACR Cryptology Conference (Crypto '99). Lecture Notes in Computer Science*, vol. 1666. – Springer-Verlag, Berlin, 1999.

[53] T. Okamoto et D. Pointcheval. – REACT : Rapid Enhanced-security Asymmetric Cryptosystem Transform. *In : RSA Cryptographers' Track (RSA '2001)*, éd. par D. Naccache. *Lecture Notes in Computer Science*. – Springer-Verlag, Berlin, 2001.

[54] T. Okamoto et D. Pointcheval. – The Gap-Problems : a New Class of Problems for the Security of Cryptographic Schemes. *In : Workshop on Practice and Theory in Public-Key Cryptography (PKC '2001)*, éd. par K. Kim. *Lecture Notes in Computer Science*, vol. 1992, pp. 104–118. – Springer-Verlag, Berlin, 2001.

[55] P. Paillier et D. Pointcheval. – Efficient Public-Key Cryptosystems Provably Secure against Active Adversaries. *In : Advances in Cryptology – Proceedings of Asiacrypt '99*, éd. par K. Y. Lam et E. Okamoto. *Lecture Notes in Computer Science*, vol. 1716, pp. 165–179. – Springer-Verlag, Berlin, 1999.

[56] H. Petersen et G. Poupard. – Efficient Scalable Fair Cash with Off-line Extortion Prevention. *In : ICICS '97. LNCS 1334*, pp. 463–477. – Springer-Verlag, Berlin, 1997. Available as technical report LIENS-97-7.

[57] D. Pointcheval. – Strengthened Security for Blind Signatures. *In : Advances in Cryptology – Proceedings of Eurocrypt '98*, éd. par K. Nyberg. *Lecture Notes in Computer Science*, vol. 1403, pp. 391–405. – Springer-Verlag, Berlin, 1998.

[58] D. Pointcheval. – New Public Key Cryptosystems based on the Dependent-RSA Problems. *In : Advances in Cryptology – Proceedings of Eurocrypt '99*, éd. par J. Stern. *Lecture Notes in Computer Science*, vol. 1592, pp. 239–254. – Springer-Verlag, Berlin, 1999.

[59] D. Pointcheval. – Chosen-Ciphertext Security for any One-Way Cryptosystem. *In : Workshop on Practice and Theory in Public-Key Cryptography (PKC '2000)*, éd. par H. Imai et Y. Zheng. *Lecture Notes in Computer Science*, vol. 1751, pp. 129–146. – Springer-Verlag, Berlin, 2000.

[60] D. Pointcheval. – Self-Scrambling Anonymizers. *In : Proceedings of Financial Cryptography '2000*, éd. par Y. Frankel. *Lecture Notes in Computer Science*. – Springer-Verlag, Berlin, 2000.

[61] D. Pointcheval. – The Composite Discrete Logarithm and Secure Authentication. *In : Workshop on Practice and Theory in Public-Key Cryptography (PKC '2000)*, éd. par H. Imai et Y. Zheng. *Lecture Notes in Computer Science*, vol. 1751, pp. 113–128. – Springer-Verlag, Berlin, 2000.

[62] D. Pointcheval et J. Stern. – New Blind Signatures Equivalent to Factorization. *In : Proceedings of the 4th ACM Conference on Computer and Communications Security*. pp. 92–99. – ACM press, New York, 1997.

[63] T. Pornin. – Optimal resistance against the Davies and Murphy attack. *In : Advances in Cryptology – Proceedings of Asiacrypt'98. Lecture Notes in Computer Science*, pp. 148–159. – Springer-Verlag, Berlin, 1998.

[64] T. Pornin et J. Stern. – Software-hardware trade-offs. *In : Advances in Cryptology – Proceedings of CHES 2000. Lecture Notes in Computer Science*, pp. 318–327. – Springer-Verlag, Berlin, 2000.

[65] G. Poupard et J. Stern. – Security Analysis of a Practical "on the fly" Authentication and Signature Generation. *In : Eurocrypt '98. LNCS 1403*, pp. 422–436. – Springer-Verlag, Berlin, 1998.

[66] G. Poupard et J. Stern. – Generation of Shared RSA Keys by Two Parties. *In : Asiacrypt '98. LNCS 1514*, pp. 11–24. – Springer-Verlag, Berlin, 1999.

[67] G. Poupard et J. Stern. – On The Fly Signatures based on Factoring. *In : Proceedings of 6th ACM-CCS*. pp. 37–45. – ACM press, 1999.

[68] G. Poupard et J. Stern. – Fair Encryption of RSA Keys. *In : Eurocrypt 2000. LNCS 1807*. – Springer-Verlag, Berlin, 2000.

[69] G. Poupard et J. Stern. – Short Proofs of Knowledge for Factoring. *In : PKC 2000. LNCS 1751*, pp. 147–166. – Springer-Verlag, Berlin, 2000.

[70] G. Poupard et S. Vaudenay. – DFC : an AES Candidate well suited for low cost smart cards applications. *In : CARDIS '98. LNCS 1820*. – Springer-Verlag, Berlin, 2000.

[71] J. Stern. – Lattices and cryptography : an overview. *In : Proceedings of PKC'98. Lecture Notes in Computer Science*, vol. 1431, pp. 50–54. – Springer-Verlag, Berlin, 1998.

[72] J. Stern et S. Vaudenay. – SVP : a flexible micropayment scheme. *In : Financial Cryptography — Anguilla, British West Indies, February 1997*, éd. par R. Hirschfeld. *LNCS*, vol. 1318, pp. 166–171. – Springer-Verlag, Berlin, 1997.

[73] J. Stern et S. Vaudenay. – CS-Cipher. *In : Fast Software Encryption, Fifth International Workshop, France, Paris, Proceedings, March 1998*, éd. par S. Vaudenay. *LNCS*, vol. 1372, pp. 189–205. – Springer-Verlag, Berlin, 1998.

[74] S. Vaudenay. – Cryptanalysis of the Chor-Rivest cryptosystem. *In : Advances in Cryptology CRYPTO'98, Santa Barbara, California, U.S.A.. August 1998*, éd. par H. Krawczyk. *LNCS*, vol. 1462, pp. 243–256. – Springer-Verlag, Berlin, 1998.

[75] S. Vaudenay. – Feistel ciphers with L_2-decorrelation. *In : Selected Areas on Cryptography, Kingston, Ontario, Canada, Proceedings, August 1998*, éd. par S. Tavares et H. Meijer. *LNCS*, vol. 1556, pp. 1–14. – Springer-Verlag, Berlin, 1999.

[76] S. Vaudenay. – On the security of CS-Cipher. *In : Fast Software Encryption, Sixth International Workshop, Roma, Italy, Proceedings, April 1999*, éd. par L. Knudsen. *LNCS*, vol. 1636, pp. 260–274. – Springer-Verlag, Berlin, 1999.

[77] S. Vaudenay. – Resistance against general iterated attacks. *In : Advances in Cryptology EUROCRYPT'99, Prague, Czech Republic, May 1999*, éd. par J. Stern. *LNCS*, vol. 1592, pp. 255–271. – Springer-Verlag, Berlin, 1999.

[78] S. Vaudenay. – Adaptive-attack norm for decorrelation and super-pseudorandomness. *In : Selected Areas on Cryptography, Kingston, Ontario, Canada, Proceedings, August 1999*, éd. par H. Heys et C. Adams. *LNCS*, vol. 1758, pp. 49–61. – Springer-Verlag, Berlin, 2000.

Autres conférences

[79] O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, R. Harley, A. Joux, P. Q. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern et S. Vaudenay. – DFC update. *In : Proceedings from the Second Advanced Encryption Standard Candidate Conference, April 1999.* – 1999.

[80] O. Baudron, H. Gilbert, L. Granboulan, H. Handschuh, A. Joux, P. Q. Nguyen, F. Noilhan, D. Pointcheval, T. Pornin, G. Poupard, J. Stern et S. Vaudenay. – Report on the AES candidates. *In : Proceedings from the Second Advanced Encryption Standard Candidate Conference, April 1999.* – 1999.

[81] H. Gilbert, M. Girault, P. Hoogvorst, F. Noilhan, T. Pornin, G. Poupard, J. Stern et S. Vaudenay. – Provable security for block ciphers by decorrelation. *In : Proceedings from the First Advanced Encryption Standard Candidate Conference, August 1998.* – 1998.

[82] M. Girault, G. Poupard et J. Stern. – Global Payment System (GPS) : un Protocole de Signature à la Volée. *In : Trusting Electronic Trade '99.* – 1999.

Thèses et habilitations

[83] L. Granboulan. – *Calcul d'objets géométriques à l'aide de méthodes algébriques et numériques : Dessins d'enfants.* – Thèse de doctorat, Université de Paris VII, Ecole Normale Supérieure, 8 déc. 1997.

[84] P. Q. Nguyen. – *La Géométrie des Nombres en Cryptologie.* – Thèse de doctorat, Université Paris 7, 1999.

[85] G. Poupard. – *Authentification d'entités, de messages et de clés cryptographique : théorie et pratique.* – Thèse de doctorat, École Polytechnique, 2000.

[86] S. Vaudenay. – *Vers Une Théorie du Chiffrement Symétrique.* – Habilitation à diriger des recherches, Université de Paris VII, Ecole Normale Supérieure, 7 jan. 1999. Disponible comme rapport LIENS-98-15.

Rapports de recherche

[87] E. Fujisaki, T. Okamoto, D. Pointcheval et J. Stern. – *RSA-OAEP is Still Alive.* – Rapport technique, Cryptology Archive ePrint 00/61, nov. 2000.

[88] L. Granboulan. – *AES : Analysis of the RefCode and OptCCode submissions.* – Rapport technique, National Institute of Standards and Technology (NIST), avr. 1999. Official Comment of the Advanced Encryption Standard Process.

[89] D. Pointcheval et S. Vaudenay. – *On Provable Security for Digital Signature Algorithms.* – Rapport technique, Ecole Normale Supérieure, 1996. Rapport LIENS-96-17.

[90] B. Preneel, A. Bosselaers, V. Rijmen, B. V. Rompay, L. Granboulan, J. Stern, S. Murphy, M. Dichtl, P. Serf, E. Biham, O. Dunkelman, V. Furman, F. Koeune, G. Piret, J.-J. Quisquater, L. Knudsen et H. Raddum. – *Comments by the NESSIE Project on the AES Finalists.* – Rapport technique, National Institute of Standards and Technology (NIST), mai 2000. Official Comment of the Advanced Encryption Standard Process.

[91] S. Vaudenay. – *A Cheap Paradigm for Block Cipher Security Strengthening.* – Rapport technique, Ecole Normale Supérieure, 1997. Rapport LIENS-97-3.

[92] S. Vaudenay. – *Provable Security for Block Ciphers by Decorrelation.* – Rapport technique, Ecole Normale Supérieure, 1998. Rapport LIENS-98-8.

Oeuvres de vulgarisation scientifique

[93] D. Pointcheval. – La règlementation en france. *Pour la Science*, n°260, juin 1999, p. 51.

[94] D. Pointcheval. – La cryptographie à l'aube du troisième millénaire. *Revue des Electriciens et Electroniciens*, mai 2001.

[95] G. Poupard et J. Stern. – Cryptologie. *Technique et Science Informatiques*, vol. 19, n° 1–2–3, 2000, pp. 409–414.

[96] S. Vaudenay. – Un réseau quantique. *Pour la Science*, vol. avr., n° 234, avr. 1997, p. 30.

Articles soumis ou en préparation

[97] O. Baudron, P.-A. Fouque, D. Pointcheval, G. Poupard et J. Stern. – Practical Multi-Candidate Election System, 2001. Submitted to PODC 2001.

[98] M. Bellare, A. Boldyreva, A. Desai et D. Pointcheval. – Key-Privacy in Public-Key Encryption, 2001. Submitted to Crypto '2001.

[99] E. Bresson, O. Chevassut, D. Pointcheval et J.-J. Quisquater. – Provably Authenticated Group Diffie-Hellman Key Exchange. – fév. 2001. Submitted to Crypto '2001.

[100] E. Bresson et J. Stern. – Proofs of Knowledge for General Exponential Formulas and Applications. – fév. 2001. Submitted to Crypto '2001.

[101] J.-S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval et C. Tymen. – Generic Chosen-Ciphertext Secure Encryption, 2001. Submitted to Crypto '2001.

[102] J.-S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval et C. Tymen. – IND-CCA2 Encryption of Arbitrary-Length Messages, 2001. Submitted to Crypto '2001.

[103] P. Fouque et J. Stern. – Fully Distributed Threshold rsa under Standard Assumptions. – jan. 2001. Submitted to Crypto '2001.

[104] E. Fujisaki, T. Okamoto, D. Pointcheval et J. Stern. – RSA-OAEP is Secure under the RSA Assumption, 2001. Submitted to Crypto '2001.

[105] D. Naccache, D. Pointcheval et J. Stern. – Twin Signatures, 2001. Submitted to Crypto '2001.

[106] P. Q. Nguyen et I. E. Shparlinski. – The Insecurity of the Digital Signature Algorithm with Partially Known Nonces. *Journal of Cryptology*, 2000. – Soumission en cours.

[107] P. Q. Nguyen et I. E. Shparlinski. – The insecurity of the elliptic curve digital signature algorithm with partially known nonces, 2001. Submitted to Designs, Codes and Cryptography.

[108] P. Q. Nguyen et J. Stern. – The Orthogonal Lattice : A New Tool for the Cryptanalyst. *Journal of Cryptology*, 2000. – Soumission en cours.

[109] J. Pieprzyk et D. Pointcheval. – Parallel Cryptography - a New Concept, 2001. Submitted to Crypto '2001.

[110] D. Pointcheval et G. Poupard. – A New NP-Complete Problem and Public-Key Identification. Submitted to Designs, Codes and Cryptography.

[111] T. Pornin. – Transparent harddisk encryption, 2001. Submission to CHES 2001.

Miscellanea

[112] O. Baudron, F. Boudot, P. Bourel, E. Bresson, J. Corbel, L. Frisch, H. Gilbert, M. Girault, L. Goubin, J.-F. Misarsky, P. Q. Nguyen, J. Patarin, D. Pointcheval, G. Poupard, J. Stern et J. Traoré. – GPS, sept. 2000. Submission to NESSIE.

[113] E. Fujisaki, T. Kobayashi, H. Morita, H. Oguro, T. Okamoto, S. Okazaki et D. Pointcheval. – PSEC : Provably Secure Elliptic Curve Encryption Scheme, sept. 2000. Submission to NESSIE and ISO.

[114] E. Fujisaki, T. Kobayashi, H. Morita, H. Oguro, T. Okamoto, S. Okazaki, D. Pointcheval et S. Uchiyama. – EPOC : Efficient Probabilistic Public-Key Encryption, sept. 2000. Submission to NESSIE and ISO.

[115] T. Okamoto et D. Pointcheval. – EPOC–3 : Efficient Probabilistic Public-Key Encryption, mai 2000. Submission to IEEE P1363a.

[116] T. Okamoto et D. Pointcheval. – PSEC–3 : Provably Secure Elliptic Curve Encryption Scheme, mai 2000. Submission to IEEE P1363a.

[117] D. Pointcheval. – HD–RSA : Hybrid Dependent RSA – a New Public-Key Encryption Scheme, oct. 1999. Submission to IEEE P1363a.

[118] T. Pornin. – Automatic software optimization of block ciphers using bitslicing techniques, 1999. Submission to FSE'99.

Géométrie et algorithmes

Composition de l'équipe

- Responsable :
  Michel Pocchiola, maître de conférences à l'ENS ;
- Doctorants :
  Pierre Angelier, allocataire moniteur, Paris 7, 09/98 ;
  Xavier Goaoc, élève de 4$^{\text{ème}}$ année, ENS Cachan, 09/00 ;
  Eric Colin de Verdière, élève de 4$^{\text{ème}}$ année, ENS Paris, 09/00.

Thèmes de recherche

L'équipe développe des travaux de base dans le domaine de la géométrie algorithmique portant sur la conception, l'analyse et la programmation d'algorithmes. Nos résultats peuvent se décliner selon deux chapitres : la géométrie des rayons et le calcul d'homotopies et d'isotopies.

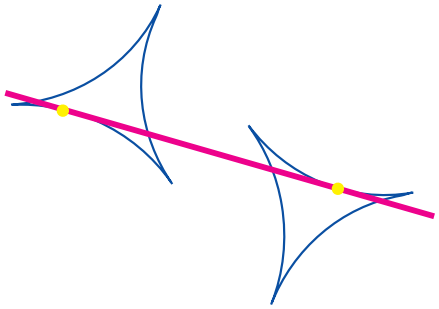

FIG. .1: La dualité pseudodroite/pseudotriangle.

Géométrie des rayons. Notre activité, de longue date dans ce domaine, se cristallise autour de l'étude du *complexe de visibilité* : un complexe cellulaire qui représente la partition de l'espace des rayons induite par une famille d'obstacles ; son étude est motivée par les problèmes géométriques de visibilité rencontrés en synthèse d'images et en planification de trajectoire. La définition du complexe de visibilité, espace topologique quotient de l'espace des rayons par la relation de visibilité entre rayons, est donnée pour la première fois dans [2]. L'algorithmique des complexes de visibilité d'objets convexes 2D (polygones, cercles, ellipses, etc) est établie dans [2, 1, 10] — introduction des mots-clés : *pseudotriangle, dualité pseudodroite/pseudotriangle, pseudo-triangulation, pseudo-triangulation gloutonne, Greedy Flip Algorithm (GFA)* — puis reprise dans [5, 6, 11]. L'objectif de cette reprise était triple :

1. Élaborer un algorithme optimal basé uniquement sur le *chirotope* des convexes c'est-à-dire l'application qui à chaque triplet de convexes associe le type combinatoire de l'arrangement dans le plan projectif des courbes des tangentes au triplet de convexes.

2. Fournir du code pour le calcul des graphes/complexes de visibilité.
3. Étudier les propriétés essentielles — à notre propos — de ce chirotope afin d'en élaborer un modèle axiomatique fini.

Le premier objectif est partiellement atteint dans [5, 6] qui présente un algorithme optimal dont la primitive de base est l'orientation relative des directions de deux bitangentes issues d'un même convexe. Ce résultat est obtenu en établissant pour les complexes de visibilité des analogues aux théorèmes dits 'de la zone' et 'de la somme des carrés' pour les arrangements de droites ; l'algorithme obtenu — construit sur le GFA — est plus simple à mettre en oeuvre et de meilleure complexité en ce qui concerne les primitives de base. Le deuxième objectif est atteint : une implémentation a été réalisé pour des polygones et pour des cercles [16, 11] et doit faire l'objet d'un module d'extension de la librairie CGAL (`http://www.cs.uu.nl/CGAL/`) dans le cadre de l'Action de Recherche Coopérative Géométrica ; cette implémentation permet égalemment de comprendre l'ensemble des notions à la base de la conception de nos algorithmes. Le troisième objectif (qui permettrait de donner plus de souplesse dans l'implémentation du GFA et en particulier dans la gestion des cas non génériques) reste à élaborer. L'un des apports conceptuels de ces travaux est l'unification sous un même formalisme, celui du GFA, de l'ensemble des algorithmes de calcul des graphes de visibilité et des algorithmes de calcul d'arrangements de droites dont en particulier la méthode de balayage topologique — Topological Sweep Method (TSM)[1]. Dans la mesure où la dualité point-droite ramène le calcul d'un arrangement de droites au calcul du graphe de visibilité d'une configuration de points le GFA se présente a priori comme une alternative à la TSM. A posteriori on peut vérifier que la TSM ainsi que ses extensions sont des instances du GFA [7, 12, 9]. Cette dernière technique fournit des algorithmes efficaces pour une grande variété de problèmes : énumérer les faces d'un arrangement d'hyperplans, déterminer les dégénérescences d'une configuration de points, construire les niveaux d'un arrangement de droites, etc. Le GFA améliore l'ensemble de ces algorithmes — simplification conceptuelle, robustesse, etc. —, et ouvre de nouvelles perspectives sur l'algorithmique des configurations de points ou, par dualité, des arrangements d'hyperplans, en dimension 3 et plus, par exemple sur le calcul par balayage d'un arrangement d'hyperplans restreint à un domaine convexe [7].

Perspectives. Dans un contexte 2D, le complexe de visibilité est à la base — directe ou indirecte — de plusieurs structures de données proposées dans la littérature pour répondre de manière efficace à diverses requêtes de visibilité utilisées dans les techniques de rendu en synthèse d'image. Citons le lancer de rayon, les calculs de vue, d'ombre et de pénombre, ou encore le

[1] H. Edelsbrunner and Leonidas J. Guibas. Topologically sweeping an arrangement. *J. Comput. Syst. Sci.*, 38 :165–194, 1989. Corrigendum in 42 (1991), 249–251.

calcul de *facteur de forme* entre éléments de surfaces. (Le facteur de forme entre deux éléments de surface est l' angle solide moyen sous lequel est vu le premier élément de surface des points du second élément de surface.) Si certaines de ces propositions ont été accompagné d'une implémentation et de tests expérimentaux aucune implémentation n'est disponible actuellement dans les bibliothèques d'algorithmes géométriques. Une de nos objectifs est de combler cette lacune afin de valider expérimentalement et de manière facilement reproductible l'ensemble des techniques déjà proposées, de tester leur intérêt dans un environnement dynamique — intérêt souvent souligné mais non prouvé — et de les adapter au problème du changement d'échelle. (Un premier travail dans cette direction a fait l'objet d'un stage de DEA [13].) Dans un contexte 3D seule la requête "calcul du facteur de forme entre un point et un élément de surface" a été étudié et exploité expérimentalement pour le rendu de scène réaliste ; l'intérêt pratique de la méthode est limité pour l'heure par les problèmes de changement d'échelle et/ou de robustesse. L'étude théorique et pratique du complexe de visibilité 3D reste très largement ouverte. Un de nos objectifs est de réaliser cette étude en s'appuyant entre autres sur l'ensemble des résultats théoriques obtenus sur la géométrie des droites de l'espace par la communauté Géométrie Algorithmique. Cruciales pour l'algorithmique des complexes de visibilité, les pseudo-triangulations sont égalemment utiles pour la détection de collision d'objets en mouvement dans le plan — nous contribuons à cette ligne de recherche par [3, 15]—, et pour la planification de trajectoires sans collision pour des systèmes articulés planaires[2] ; dans ce dernier cas un lien est établi entre la classe des pseudotriangulations et la classe des dilatations infinitésimales d'une famille de points ; c'est un développement très intéressant que nous pensons suivre de près. Pour finir nous pensons toujours à élaborer un modèle axiomatique fini des complexes de visibilité, en particulier dans l'objectif de faciliter (nous devrions probablement dire rendre possible en un temps raisonnable) l'implémentation effective de nos algorithmes.

Calculs d'homotopies et d'isotopies. Cette activité, récente pour notre équipe, procède de la volonté de nous lier à des domaines de recherche de nature plus directement appliquée. Notre point de départ est l'étude d'une méthode de métamorphose pour des objets 3D représentés par leurs bords sous forme de maillages triangulaires. La mise en oeuvre de cette méthode requiert de résoudre diverses questions relevant de la topologie algorithmique (calcul de lacets générateurs du groupe fondamental d'une surface, homotopie de lacets, etc) et de réaliser des interpolations de surfaces sans auto-intersections.

[2] R. Connelly, E. D. Demaine, and G. Rote. Straightening polygonal arcs and convexifying polygonal cycles. In *Proc. 41th Annu. IEEE Sympos. Found. Comput. Sci.*, pages 432–442, 2000. et I. Streinu. A combinatorial approach to planar non-colliding robot arm motion planning. In *Proc. 41th Annu. IEEE Sympos. Found. Comput. Sci.*, pages 443–453, 2000.

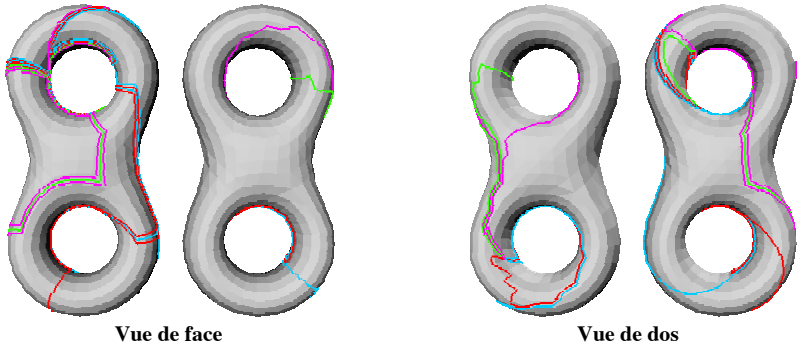

FIG. .2: Calcul des lacets sur le double tore. Sur la vue de face (resp. dos), à gauche (resp. à droite) : méthode récursive ; à droite (resp. à gauche) : méthode utilisant la réduction de Brahana.

Dans [8] nous étudions comment construire une famille *canonique* de lacets générateurs du groupe d'homotopie des lacets d'une surface de $\mathbb{R}^3$ de genre quelconque ; deux nouveaux algorithmes — simples et programmables — accompagnés de tests expérimentaux sont présentés ; le premier algorithme inverse l'opération incrémentale d'ajout d'une anse à une surface (somme connexe de surfaces) tandis que le deuxième algorithme construit un premier ensemble non canonique de générateurs puis le transforme en un ensemble canonique par une séquence de transformation de Brahana[3] ; la valorisation de ses résultats dans un module d'extension CGAL de manipulation de surfaces est envisagée. Déterminer une interpolation sans autointersection dans le cas général est un problème difficile. Le problème plus restreint de déterminer une interpolation sans auto-intersection pour deux surfaces homéomorphes à des disques semble plus abordable. Dans cette optique [14] étudie un certain type de déformation de graphes dont voici l'idée physique. Imaginons un graphe plongé dans le plan ; par la pensée, fixons les sommets et les arêtes extérieurs et remplaçons les arêtes intérieures par des ressorts ; laissons le système ainsi créé aller à sa position d'équilibre. Sous des hypothèses convenables, on peut montrer que cet équilibre constitue un plongement du graphe, c'est-à-dire qu'il n'y a aucun croisement entre les arêtes (résultat dû à Tutte[4]). Le lien entre cette approche physique des ressorts et l'isotopie est le suivant : si l'on modifie les constantes de raideur des ressorts, l'équilibre obtenu n'est pas le même ; ainsi, en faisant varier continûment les constantes

[3] T. Brahana. Systems of circuits on 2-dimensional manifolds. *Ann. Math.,* 23 :144–168,1921

[4] W. T. Tutte. How to draw a graph. *Proceedings London Mathematical Society,* 13(52) :743–768, 1963.

de raideur, on provoque une déformation du graphe. Dans [14] est réfuté une conjecture sur ce type de déformation ; on y trouve aussi une réécriture d'une preuve du théorème de Tutte, sans doute au final vraiment différente, plus lisible et plus axée sur le point de vue isotopique que l'originale.

Éléments d'évaluation

1 Collaborations

- Action de recherche coopérative Inria
  - *Vis3D*
    Début : novembre 99. Fin : novembre 01.
  - *Geometrica*
    Début : novembre 98. Fin : novembre 00.
- Projet Européen
  - Effective Computational Geometry for Curves and Surfaces, IST-2000-25006
    Début : Janvier 01. Fin : Janvier 04

2 Missions, conférences et séminaires

- Michel Pocchiola : séminaires à Bellair institute (Barbade — Janvier 2001), Bonifacio (France — Septembre 2000), Nancy-Loria (France — 1999), Paris 7 (France — 1999), Paris 6 (France — 1998), X-Orsay (France — 1998), St Etienne (France — 1998), Caen (France — 1998) ; conférences à Boston (USA — Juin 2001), Berlin (Allemagne — Mars 2001), Marseille (France — Octobre 2000), Eilat (Israel — Mars 2000), St Malo (France — Juillet 1999), Dagstuhl (Allemagne — Mars 1999), Minneapolis (USA — Juin 1998).
- Pierre Angelier : séminaires à Grasse (France — Février 2001) ; conférences à Marseille (France — Octobre 2000), Antibes (France — Mars 1999), Rennes (France — Octobre 1998).
- Eric Colin de Verdière : séminaires à Bonifacio (France — Septembre 2000) ; conférences à Marseille (France — Octobre 2000).
- Xavier Goaoc : séminaires à Bonifacio (France — Septembre 2000) ; conférences à Marseille (France — Octobre 2000).

3 Accueil de chercheurs

– **Professeurs et directeurs de recherche invités**
Gert Vegter, U. Groningen, Pays-Bas (professeur invité ENS, 2 mois 99)

4 Diffusion de la connaissance

– Groupe de travail Geometrica (action ARC, Inria) ;
– Groupe de travail Vis3D (action ARC, Inria) ;

5 Réalisation et diffusion de logiciels, brevets

– M. Pocchiola. *GFAA* est une bibliothèque d'algorithmes relatifs au Greedy Flip Algorithm un algorithme de calcul de graphes de visibilité. Développeurs : P. Angelier (98-01), X. Goaoc (00-). [16].

6 Participations à l'évaluation de la recherche

– M. Pocchiola
membre du comité de programme de ECG'00 (Eilat, Israel)

membre de la commission de spécialiste de l'INRIA Lorraine pour la campagne 2000 de recrutement CR2

7 Encadrement doctoral

Direction de thèses
– Michel Pocchiola
Pierre Angelier. *Implémentation du Greedy Flip Algorithm*, 2001 (en préparation) [11]

Participation à d'autres jurys de thèses
– Michel Pocchiola : 1 jury (rapport)

Direction de DEA
– Michel Pocchiola
Goaoc, Xavier. *Implémentation d'un algorithme de calcul de couverture polygonale.* 1999 [15]

Colin de Verdière, Éric. *Isotopies de graphes planaires avec applications à la métamorphose.* 2000 [14]

Bellanger, Eric. *Visualisation du Complexe de Visibilité.* 2000 [13]

8 Enseignement

Deuxième cycle

– Michel Pocchiola

Cours de Géométrie Algorithmique au MMFAI (99,00,01)

TD Algorithmique (98)

TD Compilation (98)

Troisième cycle

– Michel Pocchiola

Cours *Géo. Algo.* (Ecole Doctorale de Cachan, 01)

Cours *Polytopes et arrangements* du DEA Algorithmique Paris (Filière, 99,00,01)

Cours *Géo. Algo.* 3ième année ENSTA (00,01)

Cours *Recherche multidimensionnelle* du DEA Algorithmique Paris (Tronc commun, 97,98)

Cours *Introduction à la géométrie algorithmique* du DEA informatique fondamentale et applications, U. Marne la Vallée (95,96,97,98)

Publications

Articles dans des revues internationales avec comité de lecture

[1] M. Pocchiola et G. Vegter. – Topologically sweeping visibility complexes via pseudo-triangulations. *Discrete Comput. Geom.*, vol. 16, déc. 1996, pp. 419–453.

[2] M. Pocchiola et G. Vegter. – The visibility complex. *Internat. J. Comput. Geom. Appl.*, vol. 6, n° 3, 1996, pp. 279–308.

[3] M. Pocchiola et G. Vegter. – On polygonal covers. *In : Advances in Discrete and Computational Geometry*, éd. par B. Chazelle, J. Goodman et R. Pollack, pp. 257–268. – AMS, Providence, 1999, *Contemporary Mathematics*, vol. 223.

[4] M. Pocchiola et G. Vegter. – The apolar bilinear form in cagd : new applications. *In : Curve and Surface Design*, éd. par P. S. P.-J. Laurent et L. Schumaker, pp. 325–334. – Vanderbilt University Press, Nashville, TN, 2000. (Proceedings Curves and Surfaces, Saint-Malo, France, 1999.).

Communications dans des conférences internationales avec comité de lecture

[5] P. Angelier et M. Pocchiola. – On computing tangent visibility graphs. *In : Abstracts 16th European Workshop Comput. Geom.* pp. 108–111. – Ben-Gurion University of the Negev, 2000.

[6] P. Angelier et M. Pocchiola. – A sum of squares theorem for visibility complexes. *In : Proc. 18th Annu. ACM Sympos. Comput. Geom.* – 2001. to appear.

[7] P. Angelier, M. Pocchiola et S. Rivière. – On the topological sweep method. *In : Abstracts 15th European Workshop Comput. Geom.* p. 179. – INRIA Sophia-Antipolis, 1999.

[8] F. Lazarus, M. Pocchiola, G. Vegter et A. Verroust. – Computing a canonical polygonal scheme of a triangulated surface. *In : Proc. 18th Annu. ACM Sympos. Comput. Geom.* – 2001. to appear.

[9] M. Pocchiola. – Horizon trees versus pseudo-triangulations. *In : Abstracts 13th European Workshop Comput. Geom.* p. 12. – Universität Würzburg, 1997.

[10] M. Pocchiola et G. Vegter. – Pseudo-triangulations : Theory and applications. *In : Proc. 12th Annu. ACM Sympos. Comput. Geom.*, pp. 291–300. – 1996.

Thèses et habilitations

[11] P. Angelier. – *Implémentation du Greedy Flip Algorithm.* – Thèse, Ecole Normale Supérieure, 2001. En préparation.

Rapports de DEA

[12] P. Angelier. – *Comparaison experimentale du Greedy Flip Algorithm et de la Topological Sweep Method.* – DEA, Ecole Normale Supérieure, Mars/Juillet 1997.

[13] E. Bellanger. – *Visualisation du Complexe de Visibilité.* – DEA, École Normale Supérieure (Paris), 2000.

[14] É. Colin de Verdière. – *Isotopies de graphes planaires avec applications à la métamorphose.* – DEA, École Normale Supérieure (Paris), 2000.

[15] X. Goaoc. – *Implémentation d'un algorithme de calcul de couverture polygonale.* – DEA, École Normale Supérieure (Paris), 2000.

Notices descriptives, manuels d'initiation ou de référence de logiciels ou langages

[16] M. Pocchiola et P. Angelier. – *Manuel d'utilisation du GFAA*, 2001. A paraître.

Interprétation abstraite et sémantique

Composition de l'équipe

- Responsable :
  Patrick Cousot, professeur à l'ENS ;
- Autre membre permanent :
  Laurent Mauborgne, maître de conférences à l'ENS depuis sept. 2000 ;
- Doctorants :
  Jérôme Feret, élève normalien en $4^{\text{ème}}$ année, et doctorant depuis juin 2000 ;

  Antoine Miné, élève normalien en $4^{\text{ème}}$ année, stagiaire puis doctorant depuis juin 2000 ;

  David Monniaux, élève normalien de septembre 1998 à août 1999, assistant moniteur normalien à l'Université de Paris IX (Dauphine) depuis septembre 1999 ;

  Frank Védrine, assistant moniteur normalien, 9/1997 – 9/2000.

Thèmes de recherche

1 Interprétation abstraite

L'*interprétation abstraite* est une théorie de l'approximation des structures mathématiques intervenant dans la définition de la sémantique des langages informatiques, qu'il s'agisse de langages de programmation ou de langages de spécification de ces systèmes informatiques. Diverses introductions sont proposées dans [5, 6, 7].

2 Conception de hiérarchies de sémantiques par interprétation abstraite

La *sémantique* d'un programme spécifie formellement les comportements possibles d'un système informatique exécutant ce programme en interaction avec un environnement quelconque. L'interprétation abstraite offre un point de vue constructif et unificateur sur les sémantiques des langages de programmation. En effet, en faisant varier le niveau d'observation de ces comportements à l'exécution, qui peut être plus ou moins précis, l'interprétation abstraite permet de construire des hiérarchies de sémantiques intégrant toutes les sortes de sémantiques existantes ainsi que de nouvelles variantes [12, 11]. La conception de hiérarchies de sémantiques pour des familles de langages de programmation sert de fondements pour concevoir une grande variété d'analyseurs statiques pour ces langages.

3 Analyse statique par interprétation abstraite

L'application la plus connue de l'interprétation abstraite est l'*analyse statique* [9]. Si l'approximation est suffisamment grossière, l'abstraction d'une sémantique peut permettre d'en donner une version moins précise mais calculable par l'ordinateur. De ce fait un ordinateur est capable d'analyser le comportement de programmes et de logiciels avant même de les exécuter. La perte d'information ne permet pas de répondre à toutes les questions relatives à la sémantique concrète, mais toutes les réponses données par calcul

effectif de la sémantique abstraite sont toujours justes. Les applications de l'analyse statique concernent la compilation optimisante et la transformation de programmes mais principalement la mise au point et la vérification des conditions de bon fonctionnement des systèmes informatiques (comme les systèmes critiques embarqués pour le contrat européen DAEDALUS).

4 Algèbres de propriétés abstraites

Il est encore et toujours nécessaire d'étendre la gamme des analyses disponibles pour permettre de choisir le meilleur compromis entre la précision de l'analyse et son coût, en particulier pour analyser de très grands programmes (de plusieurs centaines de milliers à quelques millions de lignes). Par conséquent, une activité essentielle de l'équipe sur l'analyse statique concerne la recherche de nouvelles approximations de classes de propriétés de programmes qui soient à la fois expressives et performantes.

Cette idée se formalise par des *algèbres abstraites* utilisées pour définir des sémantiques approchées de langages de programmation dont le calcul effectif permet de déterminer automatiquement et statiquement les propriétés dynamiques d'un programme.

Une algèbre abstraite comprend d'une part un *domaine abstrait* dont les éléments représentent les propriétés abstraites considérées par l'analyse. D'autre part, une algèbre abstraite comprend des *opérations abstraites* qui formalisent la sémantique abstraite des principales primitives des langages de programmation (par exemple des approximations de transformateurs de prédicats). L'étude mathématique de la correspondance entre les algèbres de propriétés abstraites et la sémantique concrète doit être complétée par la conception de structures de données et d'opérations informatiques conduisant à une implantation en machine efficace. Ces algèbres abstraites peuvent être développées et étudiées indépendamment des langages de programmation et des analyses particulières.

Cette étude des algèbres de propriétés abstraites est particulièrement importante pour l'application pratique de l'interprétation abstraite, puisque le domaine abstrait et les structures de données utilisées pour représenter ses éléments vont déterminer à la fois la précision et la complexité des analyses. Pour une plus grande précision, les structures de données pour les domaines abstraits doivent permettre de représenter autant d'objets que possibles, et pour une meilleure complexité, ils doivent permettre de calculer efficacement les opérations abstraites associées, deux objectifs difficilement conciliables. D'autre part, les analyses les plus fines utilisent en général la possibilité d'approximer certains de ces calculs de manière dynamique à l'aide d'opérateurs d'élargissement. Ces élargissements doivent donc aussi être facilités par les structures de données des domaines abstraits.

Nous étudions également la façon de construire ces algèbres par compo-

sition d'algèbres plus simples. D'un point de vue informatique les algèbres abstraites s'implantent comme des modules et des foncteurs fournis à des analyseurs statiques génériques permettant de mettre en œuvre de nombreuses analyses et donc de réaliser de nombreuses expérimentations.

5 Algèbres de propriétés abstraites symboliques

Il s'agit de représenter des propriétés et donc des ensembles infinis d'objets informatiques symboliques (par exemple séquences, listes, arbres, graphes) eux-mêmes généralement infinis (puisqu'il faut bien prendre en compte le cas des programmes dont l'exécution ne termine pas).

En général, les structures de données classiques disponibles ne sont pas bien adaptées, et ce pour deux raisons : d'une part les opérations abstraites ne sont pas forcément celles pour lesquelles les représentations sont les plus efficaces, d'autre part les possibilités d'approximation et plus encore d'élargissement ne sont en général pas offertes. Il faut donc soit adapter les structures de données existantes en inventant des élargissements compatibles, soit inventer de nouvelles structures de données. Cette dernière voie permet d'utiliser, dès la conception des structures de données, les possibilités d'approximations sûres offertes par le cadre de l'interprétation abstraite.

5.1 Relations entre ensembles finis

Les analyses précises doivent tenir compte des liens entre les propriétés de différentes parties des programmes. Par exemple, on peut vouloir représenter les relations entre les propriétés d'entrée et celles de sortie pour fournir une analyse modulaire. Si les propriétés des différentes parties des programmes peuvent être finies, on peut utiliser des relations entre ensembles finis pour coder les liens entre les propriétés. L'avantage de cette approche est qu'il existe une manière classique et efficace de les représenter, à condition que le nombre d'ensembles à relier soit lui-même fini. Il s'agit des *diagrammes de décision binaires* (« *Binary Decision Diagrams* », BDDs), qui partagent autant que possible les sous-relations isomorphes. Ces représentations peuvent être adaptées à la représentation de fonctions d'ordre supérieur, et il est possible de définir des opérateurs d'élargissement basés sur leur taille. Ces extensions ont été appliquées avec succès à l'analyse de nécessité [15].

Lorsque les propriétés à analyser sont plus fines, comme les propriétés de terminaison ou les propriétés temporelles comme l'équité, il est nécessaire de relier un nombre infini d'ensembles. On peut dans ce cas utiliser une autre représentation classique, les automates de Büchi, mais leur complexité est trop grande vis-à-vis des opérations abstraites. Nous proposons donc une extension des BDDs, les graphes de décisions [29], qui gardent les propriétés de partage des BDDs. Les graphes de décision sont plus efficaces que les automates de Büchi, au prix d'une légère perte d'expressivité. Cette nouvelle

représentation permet d'exprimer des propriétés de vivacité ou d'équité, mais impose d'approximer les unions de relations.

5.2 Ensembles d'arbres

Les langages d'arbres permettent d'exprimer les propriétés les plus complexes, surtout lorsqu'ils contiennent des arbres infinis. On peut par exemple facilement exprimer des propriétés de traces d'exécutions concurrentes, de sécurité de protocoles crytpographiques ou encore d'état de la mémoire en cours d'exécution. Encore une fois, les représentations classiques, que ce soit par automates ou grammaires, ne sont pas adaptées à l'analyse de programmes.

Nous proposons une nouvelle représentation, fondée sur une décomposition canonique des ensembles d'arbres. Cette décomposition extrait d'une part la forme arborescente de l'ensemble, par un partage préfixe maximum, et d'autre part des relations entre les sous-arbres de cette forme arborescente [43]. La forme arborescente peut être représentée de manière très efficace par des squelettes d'arbres [30], qui partagent aussi naturellement les sous-arbres et ensembles de sous-arbres communs. Ces squelettes constituent une première approximation des propriétés, facile à manipuler et structurellement proche des ensembles d'arbres, ce qui facilite la mise au point d'opérateurs d'élargissement.

Ces représentations sont ensuite raffinées à l'aide de relations pour former des schémas d'arbres [31]. Le pouvoir expressif et la complexité de ces structures dépend du type de représentation utilisée pour les relations. En utilisant des relations finies, on peut déjà exprimer des langages hors de portée des automates classiques, comme $\{a^n b^n c^n \mid n \geq 0\}$. Avec les graphes de décision décrits plus haut, on peut facilement exprimer des preuves de terminaison sous hypothèse d'équité. La validation pratique de ces techniques devrait pouvoir être obtenue grâce à leur application dans le cadre du contrat européen DAEDALUS.

6 Algèbres de propriétés abstraites numériques

La majeure partie des programmes informatiques manipulent des variables numériques entières ou à virgule flottante. L'analyse des valeurs prises par ces variables est très importante car elle permet à elle seule de découvrir plusieurs types de bogues très répandus, comme les dépassements de tableau, les divisions par zéro ou les boucles infinies. On utilise pour cela des *domaines numériques abstraits*. Actuellement, parmi les domaines numériques abstraits existants et utilisés, on cite : le domaine des intervalles, peu coûteux (coût linéaire) mais peu précis, et le domaine des polyèdres plus précis mais très coûteux (coût exponentiel).

Dans le but d'améliorer la granularité des analyses numériques, nous avons développé deux nouveaux domaines numériques abstraits : le domaine des *différences bornées* [32] et le domaine des *octogones* [61]. Ces domaines sont basés d'une part sur une structure de données qui a déjà fait ses preuves dans le domaine de la *vérification de modèles* (« *model-checking* ») : les « *Difference-Bound Matrices* » (DBMs) et d'autre part sur l'algorithmique des graphes pondérés. Le coût (coût cubique en temps et quadratique en mémoire) et la précision de ces domaines est intermédiaire entre ceux du domaine des intervalles et ceux des polyèdres. Un point important à noter est que ces domaines sont *relationnels*, c'est-à-dire aptes à capturer des relations numériques entre plusieurs variables, ce qui n'est pas le cas du domaine des intervalles.

En pratique, ces domaines abstraits se sont révélés un bon compromis et ils ont permis des analyses hors de portée du domaine des intervalles pour un coût beaucoup plus faible que le domaine des polyèdres.

7 Analyses statiques de systèmes mobiles

De vastes réseaux de communications sont utilisés pour répondre aux besoins de notre société. Ces derniers permettent de concevoir des systèmes de processus distants, dans lesquels plusieurs processus sont exécutés en différents sites d'un réseau et interagissent en communiquant. De nouveaux processus peuvent être créés dynamiquement. De plus, ce qui est plus récent, la distribution des processus peut varier au cours du temps : c'est la programmation mobile.

Il est très difficile de prouver que le comportement d'un très gros programme est conforme à une spécification donnée. C'est encore plus délicat dans le cadre de la programmation mobile. Pourtant, nous nous devons de montrer que les systèmes mobiles que nous utilisons sont sûrs. Ainsi, dans le cadre de la téléphonie mobile, une société qui utilise un réseau de processus mobiles doit être sûre que son réseau ne demandera pas d'utiliser plus de ressources qu'elle ne peut en fournir et que les contraintes de confidentialité sur les informations qui circulent sur ce réseau ne peuvent pas être violées.

7.1 Modèles du code mobile

Avant tout, nous avons besoin d'un modèle pour décrire la mobilité et nous permettre d'isoler et de mieux comprendre les problèmes qui lui sont liés. Ces modèles servent ensuite de base à la conception de langages de haut niveau utilisables en pratique. Plusieurs modèles de la mobilité ont été proposés. Le π-calcul de Milner code implicitement la mobilité. Il met en jeu des systèmes de processus qui interagissent en échangeant des noms de canaux. Ces interactions permettent non seulement de synchroniser l'exécution des

processus, mais aussi de changer dynamiquement la distribution de ces processus. Le π-calcul est à la base du langage ERLANG que la société ERICSON a utilisé pour développer des réseaux de téléphonie mobile. Le modèle des *ambients mobiles* code explicitement la mobilité. Il représente à la fois la structure hiérarchique des sites administratifs d'un réseau, et la répartition des processus sur ces sites. En interagissant, les processus peuvent déplacer les sites dans lesquels ils sont exécutés.

7.2 Analyses statiques de code mobile

Plusieurs analyses ont été proposées pour garantir ou prouver des propriétés sur les systèmes mobiles. Elles considèrent essentiellement des propriétés de sûreté (« *safety properties* »), comme la confidentialité de l'information qui circule dans les systèmes de communication ou le nombre de processus qui sont utilisés par les systèmes. Elles consistent essentiellement à montrer que les configurations qui conduiraient à la perte de la propriété que nous cherchons à valider n'apparaissent jamais.

Nous distinguons deux types de propriétés qui suffisent à garantir l'absence de telles configurations :

- l'analyse des interférences permet de détecter quels processus sont susceptibles d'interagir parce qu'ils communiquent sur un même canal ou qu'ils sont localisés sur un même site. Nous avons réalisés une analyse des interférences à la fois dans le cas de la mobilité implicite [28] et dans celui de la mobilité explicite [59]. Ces analyses permettent de distinguer les objets créés par des instances récursives de processus, ce qui est fondamental dans l'étude de la mobilité ;
- une analyse du nombre de processus ou analyse de forme, qui permet de détecter, indépendamment des objets qui leur sont communiqués, quelle est la répartition des processus dans le système. Nous avons réalisé une analyse qui permet de compter le nombre de processus utilisés par un système mobile, dans le cas de la mobilité implicite [14]. Elle fait apparaître des exclusions mutuelles et permet de garantir le non-épuisement des ressources.

L'étude des systèmes mobiles est un enjeu important. Jusqu'à maintenant, toutes les analyses ont essentiellement porté sur des propriétés de sûreté et ne sont efficaces que sur des petits exemples. Il est indispensable de prendre en compte les propriétés de vivacité et de proposer des méthodes pour leur analyse. Il est important de passer à l'échelle industrielle et de considérer l'étude des langages réels comme ERLANG. Ceci ne peut être fait sans une analyse modulaire des réseaux, qui permette non seulement d'analyser un système morceau par morceau, mais aussi de regrouper l'information obtenue.

8 Analyses statiques probabilistes

Il est parfois nécessaire de considérer des programmes au comportement probabiliste, que ce soit pour l'étude des algorithmes probabilistes proprement dits ou pour l'étude de systèmes embarqués placés dans un environnement décrit de façon probabiliste. Dans ce dernier cas, il est en particulier intéressant d'estimer la probabilité d'atteindre des états de panne ou la probabilité que le temps d'exécution dépasse un certain seuil. Nous avons donc recherché des méthodes permettant d'obtenir par interprétation abstraite de telles estimations, ou du moins des majorants sur les valeurs considérées.

Ces recherches ont été menées avec deux objectifs :

- la réutilisation des techniques d'interprétation abstraite déjà existantes, y compris si possible au niveau de l'implantation ;
- l'exactitude mathématique de l'analyse ; en particulier, l'analyse ne devra pas introduire des hypothèses supplémentaires sur les probabilités (par exemple l'indépendance de certaines variables).

Afin de pouvoir garantir l'exactitude mathématique des analyses, nous avons dû définir des sémantiques adaptées aux programmes probabilistes et donner des relations d'abstraction ou d'équivalence entre elles. Parmi les sémantiques possibles, certaines donnent directement des possibilités d'analyse par interprétation abstraite :

- sémantique dénotationnelle en avant (suivant Kozen et [35]) ;
- sémantique dénotationnelle en arrière (adjoint linéaire de la précédente) [37].

Nous avons développé des treillis abstraits adaptés à ces sémantiques :

- sommes finies [35] ;
- localisation des mesures [35] ;
- gaussiennes ;
- queues sous-exponentielles (permettant l'analyse de terminaison de certains programmes et la validation d'analyses statistiques de temps moyens) [62].

Ces méthodes souffrent néanmoins d'une certaine complexité, aussi nous avons développé une méthode d'implantation plus simple, combinant interprétation abstraite et statistiques de Monte-Carlo [36, 63]. Cette méthode fournit des bornes supérieures d'évènements rares ainsi qu'une probabilité que cette borne soit valable. Une analyse préalable par interprétation abstraite ordinaire permet de limiter le nombre d'échantillons nécessaires à une bonne estimation. L'analyse est parallélisable avec un gain linéaire et peu de communications, ce qui permet de l'implanter sur un réseau de PC, peu coûteux par rapport à une machine parallèle conventionnelle. Cette méthode étant assez simplement adaptable à un analyseur préexistant, le CEA doit prochainement l'implanter dans son analyseur industriel Caveat.

Nous avons en outre développé un petit analyseur prototype de démonstration pour deux de nos analyses [33, 36].

9 Analyses statiques temporelles

Les analyses statiques classiques portent essentiellement sur les propriétés de sûreté (« *safety* ») ou d'invariance (comme l'absence d'erreurs à l'exécution). Au delà des propriétés de sûreté, il est maintenant fréquent de vouloir vérifier automatiquement des propriétés de programmes plus fines et donc, en général, également beaucoup plus complexes comme les propriétés temporelles [27]. L'exemple le plus connu de propriété temporelle est la vivacité (« *liveness* »), par exemple pour démontrer automatiquement la terminaison de processus parallèles équitables partageant des données communes [31].

10 Analyses statiques et vérification de modèles (« *model checking* »)

La vérification de modèles a pour limite l'hypothèse de finitude, voire la complexité pratique notamment en mémoire. L'abstraction, c'est-à-dire l'approximation par interprétation abstraite, est donc nécessaire pour la vérification de modèles infinis.

Nous avons étudié la limite des tendances actuelles de la recherche visant à automatiser l'abstraction interactivement en montrant pour les spécifications de sûreté que la découverte de l'abstraction et la preuve de la correction de l'abstraction sont logiquement équivalentes à une preuve formelle de correction de la spécification [8, 17].

Une autre tendance de la recherche en vérification de modèles est l'abstraction d'un système de transition concret par un système de transition abstrait de manière à pouvoir réutiliser les vérificateurs de modèles existants. Nous avons proposé une autre façon de procéder consistant à effectuer en parallèle une analyse statique abstraite et la vérification de modèle concret, de manière à réduire l'espace des états à explorer tout en utilisant une plus grande variété d'abstractions non forcément réduites à des systèmes de transition abstraits [13].

11 Réalisation mécanisée d'interpréteurs abstraits

Un interpréteur abstrait doit fournir un résultat sûr ; mais peut-on faire confiance à l'analyse proposée et à son implantation ? Nous avons étudié la possibilité de formaliser dans un environnement de preuve assistée par ordinateur (Coq) la correction d'un interpréteur abstrait telle qu'elle est définie par la théorie de l'interprétation abstraite. Cette correction est notamment assurée par l'usage de modules paramétriques prouvés corrects selon la spécification de leurs paramètres. En instanciant ces modules, il est possible de produire automatiquement un interpréteur abstrait certifié. Nous avons illustré cela par la production d'un petit interpréteur certifié [47].

12 Applications de l'analyse statique par interprétation abstraite

12.1 Analyse statique de protocoles cryptographiques

L'étude des protocoles cryptographiques (commerce électronique, authentification pour l'accès à un système informatique) peut se faire à deux niveau : au niveau des primitives cryptographiques ou au niveau de la correction du protocole lui-même, les primitives étant supposées vérifier certaines propriétés. Nous nous sommes intéressés à ce second aspect des choses.

Supposant idéales les primitives cryptographiques, nous exprimons les protocoles dans le modèle de Dolev-Yao, où les données échangées sont des termes sur une signature décrivant les primitives utilisées et les constantes générées. Il est alors possible de définir une sémantique des protocoles modélisant le cas d'un intrus contrôlant le réseau. S'il n'est alors évidemment pas possible dans un modèle où l'intrus a un pouvoir aussi grand de démontrer des propriétés de vivacité, il est néanmoins possible de s'assurer de la sécurité du protocole : certaines données secrètes ne doivent en aucun cas tomber en la possession de l'intrus, ou certaines machines ne doivent pas parvenir à un état marquant le bon fonctionnement tout en ayant accepté certaines données incorrectes.

Nous approchons cette sémantique par interprétation abstraite en utilisant un domaine d'automates d'arbres [33, 64]. Cette analyse a été implantée dans un prototype.

12.2 Test abstrait de logiciel

Les sociétés modernes sont très informatisées et donc hautement sensibles aux bogues dans les logiciels, en particulier ceux qui pilotent des systèmes critiques que l'on trouve dans les transports, la médecine ou le commerce électronique. Les travaux sur la vérification des logiciels sont donc très nombreux et la fiabilité et la sûreté de fonctionnement du logiciel constitue certainement une des applications principales de l'analyse statique de programmes. Cependant, toutes les méthodes automatiques de vérification de logiciels ont des limites théoriques liées aux problèmes d'indécidabilité (ce qui implique ultimement une intervention humaine) et des limites pratiques dues aux difficultés d'usage. De ce fait, le test est encore la méthode la plus utilisée pour mettre au point les programmes industriels.

Le test abstrait [10] repose sur l'idée de vérifier la correction des programmes par morceaux sur des spécifications partielles, mais en remplaçant les jeux de données par des spécifications fournies sous forme de propriétés abstraites spécifiant les comportements souhaités des programmes. Les exécutions sur ces jeux de données sont alors remplacées par des analyses statiques.

Le test abstrait étant facilement compréhensible par analogie avec les méthodes de test classiques, on peut espérer qu'il n'y aura pas de difficultés d'usage. L'intervention humaine, ultimement nécessaire, est limitée à la compréhension des algèbres abstraites utilisées à des niveaux de raffinement variés. On peut donc espérer un excellent taux de couverture pour un coût humain raisonnable, même pour de grands programmes.

12.3 Tatouage de logiciels par interprétation abstraite

Parmi les applications originales de l'analyse statique par interprétation abstraite, citons le tatouage de code mobile permettent au propriétaire d'incruster dans le code source de manière indécelable et indélébile une greffe logicielle identifiant ce composant [58]. La marque indélébile à inclure n'est pas inscrite directement dans le texte du programme, ce qui la rendrait trop facilement modifiable, mais dans le comportement à l'exécution de l'objet sans que cela altère ses fonctionnalités d'origine. Ces informations sont invisibles lors de l'utilisation de l'objet mais peuvent être extraites par analyse statique.

13 Perspectives

L'équipe travaille sur le thème de l'efficacité et de la fiabilité des systèmes informatiques qui est porteur au delà des évolutions rapides de l'informatique et vertical depuis la théorie jusqu'à, plus récemment, l'industrialisation d'abord aux USA puis en Europe. L'équipe a une visibilité internationale que traduisent les invitations, les visiteurs et les contrats. Elle participe au transfert technologique (au travers de l'essaimage des doctorants et par les contrats impliquant des industriels).

L'équipe est petite (avec deux enseignants permanents dont un depuis septembre 2000 et trois doctorants), avec un grand taux de renouvellement. L'équipe a donc des possibilités de croissance, ce qui est nécessaire pour répondre aux problèmes et satisfaire aux besoins de formation par la recherche résultant de la phase actuelle d'industrialisation de l'interprétation abstraite.

Éléments d'évaluation

1 Collaborations

– **Contrats européens :**

DAEDALUS : Validation of critical software by static analysis and abstract testing.

P. Cousot (ENS, coordinateur scientifique), R. Cousot (École polytechnique), A. Deutsch (Polyspace technologies), C. Ferdinand (AbsInt), É. Goubault (CEA), N. Jones (DIKU), A. Deutsch & D. Pilaud (Polyspace technologies), F. Randimbivololona (EADS-Airbus, coordinateur administratif), M. Sagiv (U. Tel Aviv), H. Seidel (U. Trèves) et R. Wilhelm (U. Sarrebruck).

Project IST-1999-20527 of the european 5^{th} Framework Programme (FP5), oct. 2000 – oct. 2002.

Abstract interpretation of mobile processes.

P. Cousot (ENS) et C. Priami (U. Pise). Specific research and technological development programme in the field of the training and mobility of researchers (TMR) FMBI961050, oct. 1996 – sep. 1997.

ABILE : Abstract interpretation for declarative languages.

R. Barbuti (U. de Pise), M. Bruynooghe (U. de Louvain), P. Codognet (INRIA Rocquencourt), M.-M. Corsini (U. de Bordeaux), P. Cousot (ENS), R. Cousot (École polytechnique), P. Devienne (U. de Lille), G. Filè (U. de Padoue), M. Hanus (Max-Planck-Institut für Informatik, Saarbrücken), M. Hermenegildo (U. polytechnique de Madrid), N. Jones (U. de Copenhagen), B. L. Charlier (Facultés U. de Namur), G. Levi (U. de Pise), J. Małuszyński (U. de Linköping), A. Mycroft (U. de Cambridge) et U. Nilsson (U. de Linköping).

Human capital and mobility (HCM) european network, jan. 1995 – déc. 1997.

– **Contrats bilatéraux (programmes d'actions intégrées) :**

Model-checking et analyse statique.

P. Cousot (ENS) et A. Podelski (Max-Planck-Institut für Informatik).

Programme d'actions intégrées franco-allemandes PROCOPE, jan. 2000 – déc. 2000.

Sécurité de systèmes distribués par interprétation abstraite.

P. Cousot (ENS) et R. Giacobazzi (U. Vérone).

Programme d'actions intégrées franco-italiennes GALILÉE, jan. 1999 – déc. 2000.

– **Contrats français :**

Contrats institutionnels français :

Validation de code mobile par interprétation abstraite.

P. Cousot (ENS). Projet TL97130 du programme Télécommunications du CNRS, jan. 1997 – déc. 1999.

TUAMOTU : Tatouage électronique sémantique de code mobile Java™.

P. Cousot (ENS), R. Cousot (École polytechnique) et M. Riguidel (Thales Communications).

Project RNRT 1999 n° 95, oct. 1999 – oct. 2001.

Analyses statiques probabilistes.

P. Cousot (ENS) et É. Goubault (CEA).

Contrat ENS — CEA, n° SAV 27234/VSF, jan. 1999 – déc. 2001.

Contrats industriels :

Étude des procédés de signature logicielle pour les objets mobiles écrits en Java™.

P. Cousot (ENS) et M. Riguidel (Thales Communications).

Contrat ENS — Thales Communications, jan. 1999 – déc. 2000.

La vérification statique de propriétés temporelles de logiciels avioniques par interprétation abstraite.

P. Cousot (ENS) & F. Randimbivololona (EADS Airbus).

Contrat ENS – EADS Airbus, juin 2001 – juin 2003.

– **Groupes de travail internationaux :**

P. Cousot est membre du groupe de travail WG 2.3 de l'IFIP sur la « méthodologie de la programmation ». Il participe à ses réunions de travail [39] ou les organise régulièrement en France [38].

2 Missions, conférences et séminaires

– P. Cousot :

séminaires au Max-Planck-Institut für Informatik (Sarrebruck, Allemagne – juin 1997) [72], à Obernai (septembre 1997) [38], KAIST (Taejon, République de Corée – novembre 1997) [48], Paris (janvier 1998) [68], Udine (Italie – septembre 1998) [70], Dagstuhl Seminar 99151 (Allemagne – avril 1999) [75], Paris (mai 1999) [71], Rennes (janvier 2000) [73], KAIST (Taejon, République de Corée – juin 2000) [22, 74], Montréal (Canada – septembre 2000) [66] ;

conférences Paris (septembre 1997) [9], Sydney (Australie – décembre 1997) [26], Valence (Espagne – juin 1998) [20], Pise (Italie, SAS'98 – septembre 1998), Padoue (Italie – mai 1999) [18], Venise (Italie, SAS'99 – septembre 1999), Paris (ICFP'99 & PPDP'99, septembre 1999), Osaka (Japon – novembre 1999) [21], Boston (USA, PEPM'00 – janvier 2000), Boston (USA – janvier 2000) [27], Schloß Ringberg (Allemagne – février 2000) [25], Santa Barbara (USA, LICS'00 & SAS'00 – juin 2000), Austin (USA – juillet 2000) [8, 65], L'Aquila (Italie – août 2000) [6, 10], Sarrebruck (Allemagne – août 2000) [23], Montréal (Canada, ICFP'99 & PPDP'99, septembre 1999), La Réunion (novembre 2000) [17], Santa Cruz (USA – janvier 2001) [39], Londres (UK, CW'01 & POPL'01 – janvier 2001), Redmond (USA – février 2001) [67], Munich (Allemagne – mars 2001) [24], Gênes (Italie, ESOP'01, ETAPS'01 & TACAS'01 – avril 2001) ;

cours à Taejon (République de Corée – novembre 1997) [48], Nantes (avril 1998) [51], Udine (Italie – septembre 1998) [50], Paris (IENS–X, janvier 1999) [52], Marktoberdorf (Allemagne – juillet/août 1998) [49, 56, 69], Paris (ASPROM, octobre 2000) [53].

– Jérôme Feret :

séminaires à l'École normale supérieure (mars et novembre 2000), P.P.S. (Chevaleret, janvier 2001), LORIA, Nancy (janvier 2001) ;

conférences à Pise (SAS'98, septembre 1998), Venise (SAS'99, septembre 1999), Paris (ICFP'99, septembre 1999), Paris (PPDP'99, septembre 1999), Santa Barbara (SAS'00, juin 2000) [28], State College (GETCO'00, USA, août 2000) [14], State College (CONCUR'00, USA, août 2000).

– Laurent Mauborgne :

séminaires à Paris (juin 1999) [77], Paris (janvier 2000) [80], Copenhague (Danemark – mars 2000) [78], Paris (mars 2000) [81],

Saarbrück (Allemagne – avril 2000) [82], Bruxelles (Belgique – décembre 2000) [79] ;

conférences à Pise (SAS'98, Italie – septembre 1998), Venise (Italie – septembre 1999) [29], Berlin (Allemagne – mars 2000) [30], Santa Barbara (USA – juin 2000) [31], Londres (POPL'01, UK – janvier 2001), Gênes (ETAPS'01, Italie – avril 2001) ;

cours à Copenhague (Danemark – février-mars 2000) [57] ;

séjour à Saarbrück (Allemagne – avril-mai 2000).

– Antoine Miné :
séminaire à Grenoble (novembre 2000) ;

conférence à Santa Barbara (USA – juin 2000) ;

école d'été à Cahmina (Portugal – septembre 2000).

– David Monniaux :
séminaires à Dagstuhl (Allemagne – avril-mai 2000), Londres (Royaume-Uni – avril 2000), Göteborg (Suède – juin 2000) ;

conférences à Mordano (CSFW'12, Italie – juin 1999) [34], Venise (SAS'99, Italie – septembre 1999) [33], Santa Barbara (SAS'00, USA – juillet 2000) [35], Sarrebruck (Allemagne – août 2000), Londres (POPL'01, UK – janvier 2001) [36], Gênes (ESOP'01, Italie – avril 2001) [37].

3 Accueil de chercheurs

– **Professeurs et directeurs de recherche invités**
Peter Lee (Carnegie Mellon University), juillet 1997. (Professeur invité ENS) ;

David Schmidt (Kansas State University), juin 1998. (Professeur invité ENS) ;

Reinhard Wilhelm (Universität des Saarlandes), septembre 1999. (Professeur invité ENS) ;

Andreas Podelski (Max-Planck-Institut für Informatik), mars 2000. (Professeur invité ENS) ;

Barbara Ryder (Rutgers University), mai 2001. (Professeur invité ENS).

Neil Jones (DIKU, Université de Copenhague), octobre 2001. (Professeur invité).

– **Post-doctorants**
Sven-Olof Nyström (Uppsala Universitet, oct. 1996 – sep. 1997).

Corrado Priami (Università di Pisa, oct. 1996 – sep. 1997).

Germán Puebla Sánchez (Universidad Politécnica de Madrid), octobre 1997 – décembre 1997.

Jean-François Raskin (F.U.N.D.P., Namur), octobre 1997 – décembre 1997.

Arnaud Venet (Contrat ENS — Thales Communications), mars 1999 – juillet 1999.

4 Diffusion de la connaissance

- Accueil à l'ENS du « Symposium international sur l'analyse statique », 8–10 septembre 1997.
- P. Cousot anime et organise à l'ENS le séminaire SIA « Sémantique et interprétation abstraite ». Ce séminaire accueille occasionnellement des orateurs prestigieux mais a principalement pour objet de permettre à de jeunes chercheurs français ou étrangers de présenter leurs travaux et de les voir discutés.
  Une vingtaine d'exposés ont lieu chaque année.
  `http://www.di.ens.fr/~cousot/annonceseminaire.shtml`
- Cours de formation de P. Cousot pour ingénieurs de l'industrie (Institut de l'ENS – Collège de Polytechnique [52], ASPROM [53]) ;
- P. Cousot est coordinateur scientifique du projet européen DAEDALUS (FP5/IST/-1999/-20527, oct. 2000 – oct. 2002).

5 Réalisation et diffusion de logiciels, brevets

La taille de l'équipe ne permet pas de développer des analyseurs statiques de qualité industrielle (dont le coût de développement est souvent supérieur à 25 personnes/années) et d'assurer ensuite leur maintenance et le suivi de leur évolution. Par conséquent, les logiciels développés dans l'équipe sont des prototypes dont le coût de développement est de l'ordre de quelques personnes/mois (en général 3 à 9 personnes/mois). Ces prototypes servent essentiellement à l'expérimentation nécessaire pour estimer le coût et la précision des analyses.

- P. Cousot a développé un prototype d'analyseur statique générique ainsi que divers domaines abstraits à but pédagogique [69] qui est disponible sur la toile `http://www.di.ens.fr/~cousot/Marktoberdorf98.shtml` ;
- P. Cousot et A. Venet ont développé un tatoueur de méthodes de classes Java™ dans le cadre du contrat TUAMOTU [58] ;
- J. Feret a implanté un analyseur pour les systèmes mobiles spécifiés en π-calcul [76]. Le propotype est disponible sur la toile `http://www.di.ens.fr/~feret/prototypes/` ;

- A. Miné a programmé un prototype d'analyseur statique basé sur les domaines numériques abstraits [32, 61] ;
- D. Monniaux a développé un analyseur de protocoles cryptographiques par interprétation abstraite dans un domaine d'automates d'arbres ;
- D. Monniaux a développé un analyseur de programmes probabilistes écrits dans un sous-ensemble du langage C. Cet analyseur est disponible sur la Toile en téléchargement (`http://www.di.ens.fr/~monniaux/download/absinthe.tar.gz`) et en consultation directe (`http://cgi.dmi.ens.fr/cgi-bin/monniaux/absinthe`) ;
- D. Monniaux a développé des bibliothèques d'interfaçage entre le langage Objective Caml et les librairie GMP (calcul scientifique) et Gtk ; ces bibliothèques sont mises à disposition sur la toile (`http://www.di.ens.fr/~monniaux/programmes.html.fr`) ;
- D. Monniaux a développé un classificateur d'adresses IP selon leur origine géographique utilisant des structures de données habituellement utilisées pour l'analyse de programmes.

6 Participations à l'évaluation de la recherche

- P. Cousot :

  Membre du comité de rédaction de la revue *SCP* (jusqu'en 2000) ;

  Président du comité de programme de SAS'01 ;

  Membre du comité de programme de GETCO'00, GETCO'01, SAS'99, SAS'00, WSAGV'2000 ;

  Évaluateur pour les conférences internationales ECOOP'00, ESOP'99 ESOP'00, ESOP'01, KR'00, LICS'99 PEPM'97, PLDI'01, PLI'99, POPL'97, SAIG'00, SAS'97 et SAS'98 ;

  Évaluateur pour les journaux ACM Computing Surveys, ACM TOPLAS, Acta Informatica, SCP, JACM, JASE, TCS ;

  Évaluateur pour les soumissions de projets européens IST (FP 5 RTD Programmes), autrichiens « Fonds zur Förderung der wissenschaftlichen Forschung » (FWF), italiens (Istituto Superiore Mario Boella, ISMB et « Centre International des Sciences Mécaniques » (CISM), Udine), finlandais (Finish Programme for Centers of Excellence in Research 2001–2007 de l'académie de Finlande), néerlandais « Stichting informatica-onderzoek in Nederland » (SION, the Netherlands Computer Science Research Foundation) pour le compte de « the Netherlands Organisation for Scientific Research (NWO) » ;

  Évaluateur pour le projet européen Esprit LTR project 23498 vires, Prof. P. Wolper (coordinateur) ;

Membre du conseil scientifique du département EECS du KAIST (Taeduk Science Complex, Taejon, République de Corée) ;

Expert pour le recrutement d'enseignants et chercheurs (Ben-Gurion University of the Negev (Israël), Carnegie Melon University (Computer Science Department), Imperial College of Science, Technology and Medicine de Londres (UK), Rutgers University, New Jersey, (Computer Science Department), Université de Cambridge (UK), Université de Melbourne (Australie), Université de Sarrebrück (Allemagne)).

– J. Feret :
Évaluateur pour les conférences ESOP'00, PPDP'00, ESOP'01 et SAS'01.

– L. Mauborgne :
Évaluateur pour les conférences POPL'97, FMPPTA'97, FMPPTA'98, ICCL'98, SAS'99, ESOP'00, PPDP'00, ESOP'01 et SAS'01.

– A. Miné :
Évaluateur pour les conférences ESOP'01, PADO'01 et SAS'01.

– D. Monniaux :
Évaluateur pour les conférences FMPPTA'99, FMPPTA'00, FMPPTA'01, ESOP'01 et SAS'01.

7 Encadrement doctoral

Direction de thèses

– P. Cousot :

J. Goubault, *Logique, complexité, démonstration automatique et thèmes annexes* [42], Habilitation à diriger les recherches, Université de Paris 9, Dauphine, soutenue le 27 juin 1997 ;

L. Mauborgne, *Représentation d'ensembles d'arbres pour l'interprétation abstraite* [43], Thèse de doctorat de l'École polytechnique en informatique, soutenue le 25 novembre 1999 ;

F. Védrine, *Analyses totales de programmes par l'interprétation abstraite* [44], Thèse de doctorat de l'École polytechnique en informatique, soutenue le 28 janvier 2000.

– P. Cousot et D. Parigot :

L. Correnson, *Sémantique équationelle* [41], Thèse de doctorat de l'École polytechnique en informatique, soutenue le 1er avril 2000.

– P. Cousot et A. Deutsch :
  B. Blanchet, *Analyse d'échappement, Applications à ML et Java*™ [40], Thèse de doctorat de l'École polytechnique en informatique, soutenue le 7 décembre 2000.
– P. Cousot, direction de thèses en cours : J. Feret, A. Miné et D. Monniaux.

Participation à d'autres jurys de thèses
– P. Cousot : 7 jurys dont 1 présidence et 3 rapports.

Direction de projets de DEA
– P. Cousot :
  D. Massé, *Interprétation abstraite du langage de programmation LUSTRE* [45]. 1998 ;
  D. Monniaux, *Réalisation mécanisée d'interpréteurs abstraits* [47]. 1998 ;
  A. Miné, *Représentation d'ensembles de contraintes de somme ou de différence de deux variables et application à l'analyse automatique de programmes* [46]. 2000.

8 Enseignement

Deuxième cycle
– P. Cousot :
  Directeur des études pour l'informatique à l'ENS ;
  Responsable du magistère MMFAI pour l'informatique ;
  Cours « Langages de programmation et compilation » au MMFAI [54] ;
  Cours « Sémantiques des langages de programmation » au MMFAI [55].
– L. Mauborgne :
  TDs d'algorithmique à l'École polytechnique (1997-99 et 2000-01) ;
  TDs de compilation au MMFAI (1999-2001) ;
  TDs d'algorithmique et programmation au MMFAI (1999-2001).
– A. Miné :
  Encadrement de travaux dirigés pour le cours de programmation système à l'École polytechnique (2001).
– D. Monniaux :
  Travaux dirigés et pratiques d'algorithmique et programmation en première année de DEUG MASS à l'Université Paris 9 Dauphine ;
  Participation à l'évaluation des stages en entreprise à l'École Nationale Supérieure de Techniques Avancées (1999).

Troisième cycle

- P. Cousot :
  - Cours *Fondement de l'interprétation abstraite* du DEA « Programmation : sémantique, preuves et langages ».
  - Cours de P. Cousot à des Écoles pour jeunes chercheurs [51] ;
  - Cours de doctorat de P. Cousot sur l'interprétation abstraite à l'étranger (KAIST, République de Corée [48], Université d'Udine [50], « NATO Int. Summer School 1998 on Calculational System Design » de Marktoberdorff [56]) ;
- J. Feret :
  - Participation au cours « Analyse statique par interprétation abstraite » de Radhia Cousot, dans le cadre du DEA « Programmation : sémantique, preuves et langages » (2001).
- L. Mauborgne :
  - Participation au cours« Analyse statique par interprétation abstraite » de Radhia Cousot, dans le cadre du DEA « Programmation : sémantique, preuves et langages » (1999-2001) ;
  - Cours sur les représentations d'ensembles d'arbres en analyse de programme à l'Université de Copenhague (2000) [57].
- D. Monniaux :
  - Participation au cours « Analyse statique par interprétation abstraite » de Radhia Cousot, dans le cadre du DEA « Programmation : sémantique, preuves et langages » (2001).

9 Prix et distinctions

Patrick Cousot a reçu la médaille d'argent du CNRS en 2000.

Publications

Édition d'actes ou d'ouvrages collectifs

[1] P. Cousot (éditeur). – *Proc. 8th International Static Analysis Symposium SAS'01.* – Springer-Verlag, juillet 2001, Lecture Notes in Computer Science. À paraître.

[2] P. Cousot, É. Goubault, J. Gunawardena, M. Herlihy, M. Raussen et V. Sassone (éditeurs). – *GEometry and Topology in COncurrency theory.* – Elsevier, 2001, volume 39. `http://www.elsevier.nl/locate/entcs/volume39.html`.

Chapitres de livres ou d'ouvrages collectifs

[3] P. Cousot. – The calculational design of a generic abstract interpreter. *In : Calculational System Design*, éd. par M. Broy et R. Steinbrüggen, pp. 421–505. – NATO Science Series, Series F : Computer and Systems Sciences. IOS Press, 1999, volume 173.

[4] P. Cousot. – Abstract interpretation based formal methods and future challenges, papier invité. *In : « Informatics — 10 Years Back, 10 Years Ahead »*, éd. par R. Wilhelm, pp. 138–156. – Sarrebruck, DE, Springer-Verlag, 28–31 août 2000, *Lecture Notes in Computer Science*, vol. 2000.

Articles invités

[5] P. Cousot. – Directions for research in approximate system analysis, papier invité. *ACM Comput. Surv.*, vol. 31, n° 3es, septembre 1999.

[6] P. Cousot. – Abstract interpretation : Achievements and perspectives, papier invité. *Proc. SSGRR 2000 – Advances in Infrastructure for Electronic Business, Science, and Education on the Internet*, 31 juillet – 6 août 2000.

[7] P. Cousot. – Interprétation abstraite, papier invité. *TSI*, vol. 19, n° 1-2-3, janvier 2000, pp. 155–164.

[8] P. Cousot. – Partial completeness of abstract fixpoint checking, papier invité. *Proc. 4^{th} International Symposium on Abstraction, Reformulation and Approximation, SARA '00.* Lecture Notes in Artificial Intelligence, vol. 1864, 26–29 juillet 2000, pp. 1–25. – Horseshoe Bay, TX, USA.

[9] P. Cousot. – Abstract interpretation based static analysis parameterized by semantics, papier invité. *Proc. 4^{th} International Static Analysis Symposium, SAS '97.* Lecture Notes in Computer Science, vol. 1302, 8–10 septembre 1997, pp. 388–394.

[10] P. Cousot et R. Cousot. – Abstract interpretation based program testing, papier invité. *Proc. SSGRR 2000 – Advances in Infrastructure for Electronic Business, Science, and Education on the Internet*, 31 juillet – 6 août 2000.

Articles dans des revues internationales avec comité de lecture

[11] P. Cousot. – Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. *Theoret. Comput. Sci.*, À paraître en 2001 (Version préliminaire dans [12]).

[12] P. Cousot. – Constructive design of a hierarchy of semantics of a transition system by abstract interpretation. *Electronic Notes in Theoretical Computer Science, ENTCS*, vol. 6, 1997. – `http://www.elsevier.nl/locate/entcs/volume6.html`, 25 pages.

[13] P. Cousot et R. Cousot. – Refining model checking by abstract interpretation. *Automated Software Engineering Journal, special issue on Automated Software Analysis*, vol. 6, 1999, pp. 69–95.

[14] J. Feret. – Occurrence counting analysis for the π-calculus. *Electronic Notes in Theoretical Computer Science, ENTCS*, vol. 39, 2001.

[15] L. Mauborgne. – Abstract interpretation using typed decision graphs. *Science of Computer Programming*, vol. 31, n° 1, mai 1998, pp. 91–112.

[16] L. Mauborgne. – An incremental unique representation for regular trees. *Nordic Journal of Computing*, vol. 7, n° 4, 2000, pp. 290–311.

Conférences invitées

[17] P. Cousot. – On completeness in abstract model checking from the viewpoint of abstract interpretation, conférence invitée. *In : Réunion Workshop on Implementation of Logics,* Saint Gilles, La Réunion. – 11–12 novembre 2000.

[18] P. Cousot. – Abstract interpretation and types, conférence invitée. *In : Workshop on « Static Analysis and Types »,* Palazzo del Bó, Padoue, IT. – 17–18 mai 1999.

[19] P. Cousot. – Discrete fixpoint approximation methods in program static analysis, conférence invitée. *In : 7^{th} Int. Coll. on Numerical Analysis and Computer Science with Applications, NACSA '98*, Plovdiv, BG, 13–17 août 1998.

[20] P. Cousot. – Rule-based specifications and their abstract interpretation, conférence invitée. *In : 4^{th} Advanced Seminar on Foundations of Declarative Programming, ASFDP '98.* – 15 juin 1998. Valence, Espagne.

[21] P. Cousot. – Abstraction in abstract interpretation, conférence invitée. *In : Workshop on Refinement and Abstraction,* ETL, Osaka, Japon. – 15–17 novembre 1999.

[22] P. Cousot. – An overview of abstract interpretation and program static analysis, conférence invitée. *In : 1^{st} Int. Advisory Board Workshop,* EECS Dept., KAIST, Taeduk Science Complex, Taejon, République de Corée. – 14 juin 2000.

[23] P. Cousot. – Progress on abstract interpretation based formal methods and future challenges, conférence invitée. *In : Conference at the Occasion of Dagstuhl's 10^{th} Anniversary, « Informatics — 10 Years Back, 10 Years Ahead »,* Saarland University Campus, Sarrebruck, DE. – 28–31 août 2000.

[24] P. Cousot. – Abstract interpretation for software verification, conférence invitée. *In : Workshop on Formal Design of Safety Critical Embedded Systems, FEmSys '2001,* Munich, DE. – 21–23 mars 2001.

[25] P. Cousot et R. Cousot. – Abstract testing versus abstract model-checking, conférence invitée. *In : Schloß Ringberg Seminar on « Model Checking and Program Analysis »,* organisé par A. Podelski, B. Steffen et M. Vardi. – 20–23 février 2000.

Communications dans des conférences internationales avec comité de lecture

[26] P. Cousot et R. Cousot. – Abstract interpretation of algebraic polynomial systems. *In : Proc. 6^{th} International Conference on Algebraic Methodology and Software Technology, AMAST '97*, éd. par M. Johnson. Lecture Notes in Computer Science, vol. 1349, pp. 138–154. – Springer-Verlag, 13–18 décembre 1997. Sydney, AU.

[27] P. Cousot et R. Cousot. – Temporal abstract interpretation. *In : Conference Record of the 27^{th} Annual ACM SIGPLAN-SIGACT Symposium on Principles of programming Languages, POPL '00*, Boston, MA, janvier 2000. pp. 12–25. – ACM Press.

[28] J. Feret. – Confidentiality analysis of mobile systems. *In : Proc. 7^{th} International Static Analysis Symposium, SAS '00.* Lecture Notes in Computer Science, vol. 1824, pp. 135–154. – Springer-Verlag, 2000.

[29] L. Mauborgne. – Binary decision graphs. *In : Proc. 6th International Static Analysis Symposium SAS'99*, éd. par A. Cortesi et G. Filé. Lecture Notes in Computer Science, vol. 1694, pp. 101–116. – Springer-Verlag, 1999.

[30] L. Mauborgne. – Improving the representation of infinite trees to deal with sets of trees. *In : European Symposium on Programming, ESOP 2000*, éd. par G. Smolka. Lecture Notes in Computer Science, vol. 1782, pp. 275–289. – Springer-Verlag, 2000.

[31] L. Mauborgne. – Tree schemata and fair termination. *In : Proc. 7th International Static Analysis Symposium SAS'00*, éd. par J. Palsberg. Lecture Notes in Computer Science, vol. 1824, pp. 302–320. – Springer-Verlag, 2000.

[32] A. Miné. – A new numerical abstract domain based on difference-bound matrices. *In : 2nd Symposium on Programs as Data Objects*, Lecture Notes in Computer Science. – 2001. À paraître.

[33] D. Monniaux. – Abstracting cryptographic protocols with tree automata. *In : 6th International Static Analysis Symposium, SAS'99.* Lecture Notes in Computer Science, n°1694, pp. 149–163. – Springer-Verlag, 1999.

[34] D. Monniaux. – Decision procedures for the analysis of cryptographic protocols by logics of belief. *In : 12th Computer Security Foundations Workshop.* – IEEE, 1999.

[35] D. Monniaux. – Abstract interpretation of probabilistic semantics. *In : 7th International Static Analysis Symposium, SAS'00.* Lecture Notes in Computer Science, n°1824, pp. 322–339. – Springer-Verlag, 2000.

[36] D. Monniaux. – An abstract Monte-Carlo method for the analysis of probabilistic programs (extended abstract). *In : Conference Record of the 28th Annual ACM SIGPLAN-SIGACT Symposium on Principles of programming Languages, POPL'01).* pp. 93–101. – ACM Press, 2001.

[37] D. Monniaux. – Backwards abstract interpretation of probabilistic programs. *In : European Symposium on Programming.* Lecture Notes in Computer Science. – Springer-Verlag, 2001.

Autres conférences

[38] P. Cousot. – A few remarks on the abstraction and equivalence of semantics. *In : IFIP WG 2.3, Obernai.* – 26 septembre 1997.

[39] P. Cousot. – Introduction to a discussion on mechanical formal methods for software verification. *In : IFIP WG 2.3 Santa Cruz Meeting.* – 7–12 janvier 2001.

Thèses et habilitations

[40] B. Blanchet. – *Analyse d'échappement, Applications à ML et Java*™. – Thèse de doctorat en informatique, École polytechnique, 7 décembre 2000.

[41] L. Correnson. – *Sémantique équationelle.* – Thèse de doctorat en informatique, École polytechnique, 1er avril 2000.

[42] J. Goubault. – *Logique, complexité, démonstration automatique et thèmes connexes.* – Habilitation à diriger les recherches, Université de Paris 9, Dauphine, 27 juin 1997.

[43] L. Mauborgne. – *Représentation d'ensembles d'arbres pour l'interprétation abstraite.* – Thèse de doctorat en informatique, École polytechnique, 25 novembre 1999.

[44] F. Védrine. – *Analyses totales de programmes par l'interprétation abstraite.* – Thèse de doctorat en informatique, École polytechnique, 28 janvier 2000.

Rapports de DEA

[45] D. Massé. – *Interprétation abstraite du langage de programmation LUSTRE.* – Mémoire de stage de DEA programmation : sémantique, preuves et langages, ENS, 1998.

[46] A. Miné. – *Représentation d'ensembles de contraintes de somme ou de différence de deux variables et application à l'analyse automatique de programmes.* – Mémoire de stage de DEA programmation : sémantique, preuves et langages, ENS, 2000. `http://www.eleves.ens.fr:8080/home/mine/stage_dea/index.shtml.en`.

[47] D. Monniaux. – *Réalisation mécanisée d'interpréteurs abstraits.* – Rapport de DEA programmation : sémantique, preuves et langages, Université Paris VII, 1998.

Notes de cours

[48] P. Cousot. – Workshop on abstract interpretation. – 10–15 novembre 1997. KAIST, Taeduk Science Complex, Taejon, KR.

[49] P. Cousot. – Calculational design of semantics and static analyzers by abstract interpretation. – 28 juillet – 9 août 1998. NATO Int. Summer School 1998 on Calculational System Design. Marktoberdorf, DE. Organized by F.L. Bauer, M. Broy, E.W. Dijkstra, D. Gries and C.A.R. Hoare.

[50] P. Cousot. – Corso di interpretazione astratta. – 9–12 septembre 1998. Dottorato di Ricerca, Dip. di Informatica, Univ. di Udine, IT.

[51] P. Cousot. – Interprétation abstraite. – 1er avril 1998. École jeunes chercheurs en programmation, GDR Programmation du CNRS, École des Mines de Nantes, Nantes, 23 mars – 2 avr. 1998.

[52] P. Cousot. – Analyse statique de logiciels : du test exhaustif à la vérification automatique. – 28 janvier 1999. Séminaire de formation de l'Institut de l'École normale supérieure et du Collège de Polytechnique sur l'« Analyse Statique de Logiciels », Paris.

[53] P. Cousot. – Interprétation abstraite. – 24–25 octobre 2000. Journées ASPROM sur la Sûreté des Logiciels, Paris.

[54] P. Cousot. – Langage de programmation et compilation. – 10 octobre 2000. Magistère MMFAI.

[55] P. Cousot. – Sémantique des langages de programmation. – 10 octobre 2000. Magistère MMFAI.

[56] P. Cousot et R. Cousot. – Introduction to abstract interpretation. – 28 juillet – 9 août 1998. Course notes for the « NATO International Summer School 1998 on Calculational System Design », Marktoberdorff, DE.

[57] L. Mauborgne. – Sets of trees and abstract interpretation. – février – mars 2000. Cours à l'Université de Copenhague.

Brevets

[58] P. Cousot, R. Cousot, M. Riguidel et A. Venet. – Dispositif et procédé pour la signature, le marquage et l'authentification de programmes logiciels ou matériels d'ordinateur. – Brevet en cours de dépôt.

Articles soumis ou en préparation

[59] J. Feret. – Abstract interpretation-based static analysis of mobile ambients. – Soumis à SAS '01.

[60] J. Feret. – Dependency analysis of mobile systems. – Soumis à CAV '01.

[61] A. Miné. – The octagon abstract domain, 2001. Soumis à SAS '01.

[62] D. Monniaux. – An abstract analysis of the probabilistic termination of programs. – 2001. Soumission à SAS '01.

[63] D. Monniaux. – An abstract Monte-Carlo method for the analysis of probabilistic programs. – 2001. En préparation pour soumission au journal ACM TOPLAS.

[64] D. Monniaux. – Abstracting cryptographic protocols with tree automata. – 2001. Version étendue de [33]. En cours de soumission à *Science of Computer Programming*.

Miscellanea

[65] P. Cousot. – Contribution to the panel on « Abstractions in AI and software engineering ». – 4^{th} Int. Symp. SARA '2000, Horseshoe Bay, TX, USA, 26–29 juil. 2000.

[66] P. Cousot. – Research on abstract interpretation at ENS with a few words on software abstract watermarking. – Seminar, CS Department, Mc Gill University, Montreal, Canada, 20 septembre 2000.

[67] P. Cousot. – On the design of abstractions for software checking. – 12 février 2001. Microsoft Research, Redmond, WA, USA.

[68] P. Cousot. – From semantics to types systems by abstract interpretation. – 15 janvier 1998. Séminaire AFPLC « Typages ».

[69] P. Cousot. – The Marktoberdorf '98 generic abstract interpreter. – novembre 1998. `http://www.di.ens.fr/~cousot/Marktoberdorf98.shtml`.

[70] P. Cousot. – Refining model checking by abstract interpretation. – 24 septembre 1998. Dip. di Informatica, Univ. di Udine, Italie.

[71] P. Cousot. – Interprétation abstraite et analyse statique. – 26 mai 1999. $10^{\text{ème}}$ anniversaire du LIX, École polytechnique, Palaiseau.

[72] P. Cousot. – Design of semantics by abstract interpretation. – 2 juin 1997. MPI-Kolloquium, Max-Planck-Institut für Informatik Im Stadtwald, Sarrebruck, DE.

[73] P. Cousot. – Interprétation abstraite temporelle. – 11 janvier 2000. Séminaire de l'IRISA, Rennes.

[74] P. Cousot. – Partial completeness of abstract fixpoint checking. – 13 juin 2000. ROPAS seminar, EECS Dept., KAIST, Taeduk Science Complex, Taejon, République de Corée.

[75] P. Cousot et R. Cousot. – Abstract interpretation, temporal logic and data flow analysis. – 11–16 avril 1999. Dagstuhl Seminar 99151 on Program Analysis, Schloß Dagstuhl, Wadern, Allemagne.

[76] J. Feret. – Pi s.a. : Analyse statique de code mobile par interprétation abstraite. Prototypes, `http://www.di.ens.fr/~feret/prototypes/`.

[77] L. Mauborgne. – Graphes de décision binaire. – juin 1999. Séminaire SIA de l'ENS, Paris.

[78] L. Mauborgne. – Representation of sets of trees for abstract interpretation. – 8 mars 2000. Séminaire « Internet Technologies Meetings » de l'ITUC, Copenhague.

[79] L. Mauborgne. – Representation of sets of trees for abstract interpretation. – 30 novembre 2000. Séminaire de l'ULB, Bruxelles.

[80] L. Mauborgne. – Représentation d'ensembles d'arbres. – 31 janvier 2000. Séminaire du LIAFA, Paris.

[81] L. Mauborgne. – Représentation d'ensembles d'arbres pour l'interprétation abstraite. – 13 mars 2000. ENS, Paris.

[82] L. Mauborgne. – Sets of trees and abstract interpretation. – 11 avril 2000. Séminaire du MPI, Sarrebruck.

[83] D. Monniaux. – The Absinthe abstract interpreter. Prototypes, `http://cgi.dmi.ens.fr/cgi-bin/monniaux/absinthe`.

[84] D. Monniaux. – Efficient storage for storing the country of internet protocol domains. – 2001.

Langages, types et logique

Composition de l'équipe

- Responsable :
  Giuseppe Longo, directeur de recherches (DR1) CNRS ;
- Autres membres permanents :
  Giuseppe Castagna, chargé de recherche CNRS ;
  Maribel Fernandez, maître de conférences à l'ENS ;
- Post-doctorants :
  S. Egger, boursier Univ. Oxford, 9/99–9/00 ;
- Doctorants :
  Frédéric De Jaeger, allocataire moniteur normalien, ENS - Paris 7, 9/99–9/02 ;
  Lionel Khalil, École Polytechnique, 9/99–9/02 ;
  Gabrile Santini, allocataire moniteur, Paris 7, 9/97–9/00 ;
  Francesco Zappa Nardelli, allocataire moniteur, Paris 11, 9/00–9/03 ;
  Silvia Crafa, boursière de doctorat, Université de Venise, 9/00–9/01.

Thèmes de recherche

Les recherches conduites au sein de cette équipe trouvent leurs racines communes dans l'étude des systèmes logiques de Types et de leur sémantique. Depuis les années '70 ces systèmes ont donné lieu à une grande variété d'applications informatiques allant de la conception de langages de programmation à l'analyse et synthèse de programmes et leur spécification formelle, jusqu'à la déduction automatique.

À partir de cette base commune cohérente, l'activité de recherche de cette équipe a su évoluer et trouver sa propre forme de verticalité théorie-applications, évoquée dans l'introduction de ce rapport, grâce aux différents apports de trois chercheurs désormais tout à fait autonomes.

Ainsi des recherches théoriques sur les langages logico-algébriques côtoient les extensions de langages commerciaux tels que Java ou O_2 ; des études fondamentales sur l'intégration de différents paradigmes de programmations sont menées parallèlement à celles portant sur l'architecture de sécurité de la Java Virtual Machine et la détection statique d'attaques ; des réflexions sur les structures géométriques dans la déduction cohabitent avec les applications des réseaux de preuve en Logique Linéaire et l'expérimentation de primitives de mobilité implementées sur différentes platformes et utilisées dans deux applications commerciales récentes.

Loin de s'étouffer réciproquement, la diversité et la verticalité de nos recherches en constituent une richesse et un atout. En partant d'une base commune, au moins quatre thèmes de recherche se sont développés au sein de cette équipe. Ces thèmes, qui veulent s'inscrire à plein titre dans l'évolution de notre laboratoire, sont : les modèles de calcul multiparadigmes, la programmation orientée objets, la mobilité dans les systèmes distribués et le rôle de l'espace dans le calcul et dans l'analyse des racines cognitives du raisonnement.

Équipe Langages, types et logique

1 Modèles de calcul multiparadigmes et réseaux d'interaction

Un premier axe de recherche de l'équipe porte sur l'étude des modèles de calcul des langages de programmation déclaratifs traditionnels (algébriques, fonctionnels, logiques, orientés objets), et leurs combinaisons (modèles multiparadigmes). Il existe plusieurs langages de programmation multiparadigmes réalistes (cf. Java) ; nous développons des modèles de calcul multiparadigmes dans le but d'obtenir une base formelle permettant l'étude des propriétés calculatoires de ces langages, ainsi que la définition de nouveaux langages avec des bonnes propriétés.

Les langages algébriques (appelés aussi équationnels) dont on peut citer par exemple OBJ, ont un mécanisme d'évaluation fondé sur la simplification d'expressions (réduction). Dans le cas des langages fonctionnels, le modèle de calcul traditionnel est le λ-calcul. Dans les langages logiques, un programme est un ensemble de clauses sur un ensemble de prédicats et le modèle d'exécution est défini par le principe de résolution, qui se spécialise en surréduction (" narrowing " en anglais) dans le cas du prédicat d'égalité. Dans les langages orientés objets, les programmes sont des ensembles d'objets avec lesquels on peut calculer grâce à des méthodes que l'on peut invoquer ou mettre à jour.

Tous ces langages, bien qu'universels, se sont avérés être bien adaptés à la résolution de problèmes dans certains domaines spécifiques. Cette constatation a ouvert les portes à la quête d'un paradigme de programmation combinant les principaux avantages de chaque style. Nous remarquons que dans tous ces langages, la réécriture joue un rôle principal dans la définition des modèles de calculs associés. C'est grâce à cette base commune qu'il est possible de les combiner de manière uniforme, mais les propriétés de ces langages multiparadigmes (ou plutôt de leurs modèles de calculs) ne sont pas directement la somme des propriétés de leurs constituants : divers problèmes, appelés problèmes de *modularité*, apparaissent (une propriété est dite modulaire si elle est vraie pour un système quand elle est vraie pour chacun de ses constituants). Nous avons étudié quelques-uns de ces problèmes dans les langages multiparadigmes. Les systèmes de types se sont avérés être un outil précieux dans l'étude des propriétés de modularité. Nous avons développé plusieurs systèmes de types pour les langages fonctionnels, algébriques, orientés objets, et leurs combinaisons.

Nous nous intéressons aussi aux aspects pratiques, liés à l'implèmentation, de ces langages multiparadigmes. Nous avons choisi les réseaux d'interaction de Lafont (dérivés des réseaux de preuve de la logique linéaire) comme langage d'implémentation, car ils permettent une analyse fine des calculs et du partage (ils ont permis en particulier le codage de l'algorithme de réduction optimal dans le λ-calcul). Nous avons obtenu plusieurs codages des langages fonctionnels et algébriques dans les réseaux. Nous signalons qu'il

existe plusieurs implémentations, séquentielles et parallèles, des réseaux d'interaction, donc un codage d'un langage de programmation dans les réseaux donne directement une implémentation de ce langage.

Langages algébrico-fonctionnels

Dans le paradigme algébrico-fonctionnel (mélange des styles algébrique et fonctionnel) les propriétés de terminaison et de confluence sont cruciales, puisqu'elles assurent l'existence d'un résultat unique pour chaque programme. En collaboration avec F. Barbanera et H. Geuvers [14], nous avons obtenu des conditions suffisantes de modularité de la terminaison dans l'extension algébrique du λ-cube. Ce résultat a été postérieurement étendu à des règles de réécriture plus générales par F. Blanqui dans son stage de DEA que j'ai codirigé avec J-P. Jouannaud. Nous avons aussi obtenu des résultats de modularité pour la normalisation et la normalisation de tête [13].

Également en collaboration avec S. van Bakel et F. Barbanera [30] nous avons montré que la terminaison reste modulaire si l'on combine non seulement les langages algébriques et les langages fonctionnels mais aussi les systèmes de types intersection et de types universellement quantifiés (Système F). Nous montrons l'intérêt d'utiliser des types de rang 2, qui définissent un système décidable et, en plus, ont l'avantage par rapport à d'autres systèmes plus populaires comme celui de ML, d'avoir des jugements de type canoniques. Ces travaux ont été réalisés dans le cadre du projet NATO International Scientific Exchange Program "Extended Rewriting and Types". L'étude de ce paradigme est un des objectifs du groupe de travail " Mélanges de systèmes algébriques et de systèmes logiques ", que M. Fernández anime avec D. Kesner et R. Di Cosmo.

Langages algébriques orientés objets

Les langages algébriques orientés objets sont obtenus en mélangeant les styles de programmation algébrique et par objets. En collaboration avec A. Compagnoni [37] nous avons défini un langage de cette famille en combinant le ς-calcul de Abadi et Cardelli avec la réécriture algébrique. En collaboration avec F. Barbanera et A. Compagnoni nous travaillons actuellement sur la définition d'un calcul général combinant objets, λ-calcul et réécriture.

Langages logico-algébriques

Dans le cas du mélange de styles logique et algébrique, nous nous sommes concentrés sur les problèmes de résolution de diséquations (E-disunification) et leurs généralisations aux problèmes de complément et d'élimination de la négation [17]. L'étude des propriétés du mélange algébrique, fonctionnel et logique fait partie de nos projets de travaux futurs.

Le paradigme d'interaction

Dans le but d'utiliser les réseaux d'interaction pour l'implémentation des langages algébrico-fonctionnels nous avons étudié en collaboration avec I. Mackie les relations entre systèmes de réécriture et réseaux [19]. Nous avons montré que les réseaux peuvent coder seulement une classe de systèmes de réécriture (séquentiels) et ceci nous a amené à définir une généralisation parallèle des réseaux. Nous étudions actuellement d'autres généralisations dans le cadre du projet CNRS/NSF "Logic based specification and verification tools for concurrent languages" en collaboration avec des chercheurs de l'INRIA et de l'Université de Pennsylvanie. L. Khalil a commencé en septembre 1999, sous la direction de M. Fernández, une thèse sur ce sujet.

L'étude des codages des langages fonctionnels dans les réseaux nous a permis d'obtenir un résultat dans un domaine lié : les calculs de substitutions explicites. Nous avons défini un λ-calcul avec substitutions et gestion de ressources explicites, confluent et préservant la normalisation forte [40]. De plus, ce calcul nous permet de simuler les stratégies d'appel par valeur, par nom, et par nécessité.

Les réseaux d'interaction peuvent également être considérés comme un paradigme de programmation déclaratif. De ce point de vue nous nous intéressons en particulier aux systèmes de types pour les réseaux. Nous avons étendu le système de Lafont, rajoutant du polymorphisme au niveau des données et types intersection [18]. L. Khalil, dans son stage de DEA réalisé sous la direction de M. Fernández, a étudié un autre aspect du polymorphisme : quand les ports des agents peuvent être utilisés soit comme entrée, soit comme sortie, selon le contexte [43].

Une autre propriété importante de ce point de vue, étudiée en collaboration avec I. Mackie, est l'équivalence de comportement des programmes dans les réseaux. Nous avons d'abord étudié cette propriété pour les réseaux typés [38], et donné une caractérisation co-inductive de l'équivalence qui a de nombreuses applications, en particulier pour l'optimisation de systèmes de réseaux d'interaction. Pour faciliter l'étude de la sémantique opérationnelle des réseaux nous avons défini un calcul d'interaction [39] qui permet de donner une base formelle aux implèmentations. Il nous a permis d'étendre les résultats de [38] sur l'équivalence opérationnelle aux réseaux non-typés [41].

2 Typage des langages objets et des fonctions surchargées

La recherche effectuée au sein de l'équipe sur les langages objets et des fonctions surchargées s'inscrit dans le cadres d'un axe de recherche démarré par notre équipe en 1992. C'est dans un tel cadre que nous avons approfondi l'étude des fonctions surchargées (démarré dans la thèse de doctorat de G.

Castagna) en définissant un formalisme qui unifie lambda-abstractions et fonctions surchargées [15].

En collaboration avec John Boyland (Berkeley et Carnegie Mellon) nous avons montré l'application pratique des résultats théoriques obtenus auparavant sur la covariance et la contravariance. Plus précisément nous avons défini une extension conservative du langage de programmation Java par des multi-méthodes sans enfreindre les caractéristiques principales de ce langage qui sont la modularité et la compilation séparée [31]. Nous avons développé un prototype de ce système basé sur la version pour Solaris du compilateur 1.1.2 de Java, ce qui constitue la première implémentation de multi-méthodes dans un langage "à la Simula".

En ce qui concerne la théorie des types et la démonstration automatique, nous avons défini un calcul avec types dépendants, sous-typage et surcharge à liaison tardive [16]. Outre son intérêt théorique ce travail est motivé par plusieurs besoins pratiques qui varient de la définition de codages logiques, à la spécialisation et réutilisations de preuves, à l'extension orientée objets du système de modules de SML. La difficulté de l'étude théorique nous a amené à définir un nouveau système de sous-typage pour les types dépendants qui améliore en nombreux points les systèmes existants.

Actuellement notre intérêt dans ce secteur ne porte pas sur les langages objets eux mêmes, mais sur l'apport que ces langages peuvent fournir, tant aux niveaux de fonctionnalités que comme base expérimentale, à l'étude des l'étude de la mobilité telle que nous la décrivons dans la prochaine section.

3 Programmes Mobiles et Sécurité

Les données, en tant que ressources sensibles doivent être *sûres* et *sécurisées* : sûres dans le sens oú elles doivent posséder certaines propriétés qui en assurent la correction et la fiabilité ; sécurisées dans le sens oú elles doivent être gérées de manière à empêcher toute utilisation malveillante ou non autorisée.

Les travaux détaillés dans la section précédente sont la continuation ou l'aboutissement des thèmes de recherche démarrés auparavant, et ils sont centrés autour du typage. Or le typage, quoique ingrédient indispensable à la production de logiciel de qualité, ne couvre que l'aspect sûreté, et touche seulement de manière marginale la sécurité. En outre, la dissémination croissante des données ainsi que l'expansion d'Internet posent de nouveaux enjeux en matière de sécurité, tout spécialement en présence de programmes mobiles.

C'est pourquoi depuis 1998 nous avons ouvert un nouvel axe de recherche de manière à inclure les aspects de sécurité en particulier en présence de computations mobiles sur des réseaux à grande échelle (Wide Area Networks). L'approche suivie est celle que nous avons déjà utilisée auparavant pour étu-

dier les langages objets. Plus précisément, en partant d'un certain nombre de problèmes concrets, nous avons défini un cadre formel dans lequel étudier ces problématiques. En particulier avec Jan Vitek (Purdue University) nous sommes partis de problèmes de sécurité de l'application "HyperNews" qui était en développement à l'université de Genève. Cette application devait gérer la distribution payante de documents à brève durée de vie (tels que des dépêches d'information) sur Internet. Nous avons donc défini un modèle formel de programmation mobile, le Seal Calcul [36], dont les primitives ont été utilisées pour développer une plateforme d'agents mobiles sur Java, nommé JavaSeal, sur laquelle l'application HyperNews a été ensuite développée ainsi qu'une deuxième application commerciale pour "registars".

En utilisant le Seal Calcul comme point de départ, nous avons commencé à explorer de nombreux aspects de la mobilité. Nous avons coencadré avec Isabelle Attali et Denis Caromel (équipe Oasis à l'INRIA Sophia-Antipolis) un stage de DEA portant sur les aspects d'implémentation de la mobilité dans l'environnement distribué ProActive [47]. Avec Jan Vitek nous avons utilisé le Seal Calcul comme langage de spécification pour caractériser un ensemble d'attaques qu'un serveur peut porter à l'encontre de ses clients [44]. Nous avons encadré un stage de DEA pour étudier le typage du Seal Calcul, et caractériser la notion d'interface d'un agent mobile [57] ; ce travail actuellement se poursuit en collaboration avec Giorgio Ghelli (Université de Pise) et dans le cadre de la thèse de Francesco Zappa et porte sur l'exploration de différentes notions d'interactions entre agents mobiles et sur l'application de la théorie développé au typage de la platforme JavaSeal. Enfin, avec Véronique Benzaken de l'Université de Paris XI nous avons coencadré un stage de DEA sur l'utilisation de la mobilité à la Seal Calcul pour le commerce électronique [49].

La recherche centré sur le Seal calcul ne constitue que la moitié de notre effort de recherche sur la mobilité. En fait dans le cadre de thèse de Michele Bugliesi et de Silvia Crafa nous avons exploré d'autres aspects et d'autres formalismes liés à la mobilité et à la sécurité. En particulier un travail de détection de "chevaux de Troye" dans les ambients mobiles a conduit (de manière assez inattendue) à une justification formelle de l'architecture de sécurité de la Java Virtual Machine [33, 34]. Parallèlement nous avons exploré l'intégration et le typage des objets dans les systèmes mobiles [32, 35]. Actuellement nous tachons de comprendre comment des concepts et des modèles classiques de sécurité s'intègrent dans un cadre de mobilité.

Hors du cadre de la mobilité mais toujours dans le domaine de la sécurité et sûreté des données, nous avons démarré une étude de la vérification des contraintes d'intégrité et coencadré un stage de DEA portant sur l'ajout et la vérification statique de ces contraintes en Java [49].

Enfin dans ce courant s'inscrit la tenue du cours de DEA "Sûreté, Intégrité et sécurité des données" dont G. Castagna est co-responsable et qui se tient dans le DEA I3 (Information, Interaction, Intelligence) de l'Université Paris

XI.

4 Polymorphisme et Preuves

Paramétricité et soustypage

L'étude des liens entre paramétricité, soustypage et héritage est à la base de la collaboration de K. Milsted (CNET, France Télécom) et S. Soloviev (Durham Univ. et, ensuite, Univ. de Toulouse) avec G. Longo. Ces recherches sont en continuité avec les activitées menées depuis lontemps dans l'équipe. Leur retombé principale a été une analyse du polymorphisme dans les langages fonctionnels de programmation qui a permis de mettre en évidence l'importance pratique d'un aspect du polymorphisme qui n'avait pas eu assez d'attention du coté théorique : le polymorphisme "ad hoc". Ce dernier est en fait une forme de "paramétricité" qui est très bien exprimée par les systèmes de types du second ordre, largement utilisé en programmation, pourvue que l'on arrive à la rendre compatible avec des systèmes de "soutypage". Le traitement unifié du polymorphisme, comme système du second ordre, et du soustypage, comme forme d'implication logique minimale, nous a ammené à developper des extensions des systèmes fonctionnels classiques qui les enrichit par des formes uniformes et mathématiquement cohérentes de polymorphisme ad hoc. Des développements récents de ces systèmes se trouvent dans [21] et [22] : on y propose un calcul des séquents "parfaitement expressif", c'est à dire complet par rapport aux propriétés de la notion de soustype dans les langages fonctionnels.

Cette approche a permis en particulier de développer un thème qui est au coeur des rapports entre Programmation Fonctionnelle et "Programmation Orientée Objets" : le traitement fonctionnel de notions comme le "passage de message" et la "surcharge".

Preuves Prototypes

Une analyse originale du "niveau d'invariance" des preuves est proposé par la notion de Preuve Prototype, en Théorie des Types. Il s'agit de comprendre quel est le "squelette" d'une preuve ou ce qui la rend invariante par rapport à la généricité des ses arguments/variables. L'idée est originale, par rapport à l'accent, mis en Théorie de la Preuve et, par conséquent, en Démonstration Automatique, sur l'induction, comme seul principe de preuve (arithmétique). Le preuve prototypes, au contraire, sont au coeur de la patique mathématique et, à cause des théorèmes d'incomplétude, elles paraissent incontournables aussi en Artihmétique (voir [29]). La Théorie des Types permets de les introduire avec rigueur et de démontrer que la notion ainsi obtenue est "cohérente" et "décidable" (voir [42] et [20]).

Epistémologie et Sciences Cognitives

La mise en place du CenECC de l'ENS ("Centre interdépartemental pour les Systèmes Complexes et la Cognition", voir dessous), est le résultat d'un engagement, de plus en plus important, dans une réflexion interdisciplinaire centrée, en particulier, sur le "problème de l'intelligibilité géométrique de l'espace". Ce problème "traverse" différentes discipline et se pose aujourd'hui aussi en Informatique (voir "Geometry in concurrency" numero special de MSCS, revue de la Cambridge Univ. Press dirigé par G. Longo).

Les premiers articles sur ces sujets (et sur des thèmes proches) constituent une réflexion sur le continu (de l'espace et du temps) et l'infini mathématique ainsi que sur leurs formalisations logiques et computationnelles, [9], [10]. Le rôle de l'action et du mouvement dans la constitution de l'espace sensible est mis en évidence dans [6] (voir aussi [25], [24], [23], [26], [28]).

Un dialogue avec des biologistes et des physiciens est au coeur de ces activités. En effet, deux Groupes de Travail, l'un sur les Fondements des Mathématiques et de la Physique (CeSEF), l'autre en Géométrie et Cognition sont devenus une composante importante de ces activités scientifiques : le premier vient de compléter un volume pour Kluwer (voir l'article [11]) ; l'autre est le point de départ d'un nouveau projet de recherche (voir dessous).

5 Perspectives de recherche

Modèles de calcul multiparadigmes et réseaux d'interaction

Dans le but d'avancer vers la définition et l'implémentation d'un langage de programmation déclaratif multiparadigme, nous avons étudié plusieurs paradigmes de programmation (équationnel, fonctionnel, logique, orienté objets, d'interaction) et quelques-unes de leurs combinaisons. Dans chaque cas, nous nous sommes concentrés sur : la définition du modèle de calcul associé ; la conception de systèmes de types permettant d'assurer les propriétés souhaitées pour ces langages (confluence ; dans certains cas terminaison, normalisation, ou simplement normalisation de tête ; modularité ; etc) ; la définition d'une sémantique dénotationnelle ou opérationnelle, et dans le cas des réseaux d'interaction, le développement de techniques de preuve permettant de montrer l'équivalence de programmes. Il reste bien sûr encore de nombreux problèmes à résoudre, tant du point de vue théorique que pratiques :

1. En ce qui concerne les langages fonctionnels, nous nous sommes concentrés sur l'étude d'un calcul de substitutions explicites qui modélise la stratégie d'évaluation close. Ce calcul est dérivé d'une implèmentation du λ-calcul basée sur les réseaux d'interaction. Nous avons comparé de manière empirique cette stratégie, la stratégie optimale, et la stratégie faible, et nous avons remarqué que la stratégie close est proche de l'optimale en nombre de β-réductions, et souvent meilleure quand

on considère le nombre total d'opérations réalisées. Elle est également plus efficace que les stratégies faibles. Toutefois, ces résultats n'ont pas encore été justifiés du point de vue théorique, nous travaillons actuellement dans cette direction.

Comme les réseaux d'interaction, la Géométrie de l'interaction (dérivée de la Logique Linéaire) s'est avérée être un outil très puissant pour le développement d'implémentations du λ-calcul. Toutefois, ce domaine de recherche très prometteur n'a pas encore été étudié de manière exhaustive : jusqu'à maintenant toutes les machines abstraites développées à partir de la Géométrie de l'interaction suivent une stratégie d'appel par nom. Nous travaillons actuellement sur une machine qui implémente l'appel par valeur.

2. En ce qui concerne les combinaisons de réécriture et λ-calcul, nous aimerions avancer vers l'implémentation d'un langage algébrico-fonctionnel avec inférence de types tant sur les définitions algébriques que sur le λ-calcul. Le système avec intersection et quantification universelle de rang 2 est un bon candidat.

   D'autre part nous nous intéressons aux aspects sémantiques de ces langages, plus précisément, le développement de modèles dénotationnels ou opérationnels permettant d'étudier des propriétés comme l'équivalence de programmes. L'approche modulaire semble bien adaptée à ce problème.

   Ces projets de recherche s'intègrent de façon naturelle dans le groupe de travail (PRC GDR ALP) " Mélanges de systèmes algébriques et de systèmes logiques " auquel nous participons.

3. Dans le cas des langages orientés objets, notre contribution concerne seulement les aspects de modularité de la confluence quand on combine réécriture et objets. L'ajout du λ-calcul ne semble pas poser de nouveaux problèmes. Les points sur lesquels nous travaillons encore sont la définition d'un calcul plus puissant que le ς-calcul, permettant l'extension dynamique des objets, et la caractérisation de la propriété de terminaison.

4. Finalement, en ce qui concerne le paradigme d'interaction, nous travaillons actuellement sur deux axes de recherche : d'une part, l'obtention d'une implémentation efficace des langages algébrico-fonctionnels, d'autre part, la modélisation du parallélisme, et plus précisément des calculs de processus. Ces projets de recherche s'intègrent naturellement dans deux projets internationaux auxquels nous participons : le réseau européen TMR " Linear Logic in Computer Science ", et le projet CNRS/NSF " Logic based specification and verification tools for concurrent languages ".

Mobilité et securité

Le recherche sur la mobilité n'est qu'à ses débuts. C'est pourquoi notre plan de recherche s'articule en plusieurs directions que nous comptons poursuivre en même temps :

1. *Aspects théoriques :* les calculs de mobilité actuell, parmi lequels le Seal Calcul doivent être peaufinés afin de mieux gérer les problèmes de mobilité en présence de duplication des agents mobiles (en particulier le traitement des canaux publics). La théorie de l'équivalence doit être développée ainsi qu'une bonne notion d'observation pour l'instant insuffisante. Il y a en plus tout un ensemble d'aspects pratiques de la mobilité dont l'étude formelle n'est qu'à ses premiers balbutiements : tel est le cas de l'utilisation et du rapport entre synchronie et asynchronie, de la tolérance aux fautes, de la qualité de service et ainsi de suite. Tout ceci peut passer par la redéfinition des calculs de mobilité actuels ou de leur refonte dans d'autres paradigmes de modélisation.
2. *Aspects vérification :* Cet aspect est étroitement lié au point précédent. Une fois les bonnes notions d'équivalence et d'observation définies nous nous attellerons à prouver (de manière automatique si possible) des propriétés de sécurité des spécifications. Nous envisageons d'explorer plusieurs solutions, telles que le model checking, l'analyse de flux, l'interprétation abstraite, etc.
3. *Aspects spécification :* L'utilisation de Seal comme langage de spécification comporte deux volets orthogonaux. D'une part nous essaierons d'utiliser le Seal pour définir de manière précise et formelle certaines concepts "universels" de la programmation mobile et plus généralement distribuée. D'autre part, nous essaierons de spécifier en Seal des systèmes distribués existants, afin d'en étudier les propriétés de sécurité (s'inscrivent dans ce cadre le deux stages de DEA co-encadrés un portant sur la spécification en Seal d'un système de commerce électronique sur le Web basé sur des agents mobiles, et l'autre sur la spécification toujours en Seal du système ProActive, une bibliothéque Java qui implémente la distribution de manière transparente).

   Indépendamment du Seal Calcul nous sommes en train de monter une collaboration avec la Boston University et l'Université d'Alexandrie pour étendre les systèmes de types pour les calculs mobiles afin de les appliquer au applications "network-aware" pour pouvoir estimer la fiabilité (*reliability*) des connections et la qualité de service (QoS).

   Tout ceci devrait nous donner un bon aperçu des besoins du secteur et des eventuels problèmes recontrés, et nous comptons utiliser cette experience comme base de depart pour peufiner les aspects traiteś aux points précédents.
4. *Aspects typage :* Un autre aspect important est celui du typage du Seal

calcul que nous avons commencé à attaquer en collaboration avec Giorgio Ghelli de l'Université de Pise. L'aspect typage pourrait et devrait avoir des répercussions sur tous les points précédents car, en présence de typage, la définition d'équivalence et les preuves de propriétés résultent en général simplifiées.

5. *Aspects implémentation :* Les spécifications en Seal ou en tout autre formalisme de mobilité ne doivent pas rester au niveau abstrait mais doivent être facilement implémentables. C'est pourquoi nous envisageons d'explorer différentes possibilités d'implémentation de primitives de mobilité, commea été déjà fait pour la prémiere version du Seal Calcul avec la definition de la platforme JavaSeal.

Tous ces aspects tendent à un but unique qui constitue notre perspective de recherche à long terme : la définition d'un modèle de computation globale point de départ pour la définition de paradigmes de programmation d'applications mobiles sur des systèmes largement distribués. La caractéristique principale de ces application serait que leurs propriétés de robustesse, de sûreté et de sécurité seraient garanties par le modèle même ou bien aisément vérifiables par une analyse statique. C'est dans cette perspective que nous avons crée et/ou nous sommes en train de monter plusieurs collaborations notamment avec l'université de Sussex, l'Université de Venise, l'Université de Turin, Microsoft Research Europe, la Boston University, la Purdue University, et l'Université d'Alexandrie.

Calculabilité sur les réels

La Théorie des domaines paraît fournir des outils originaux pour une analyse en termes de calculabilité de notions et secteurs très importants des Mathématiques : les fonctions et fonctionelles réelles et la Théorie de la Mesure. Deux thésards travaillent actuellement sur ces thèmes.
On peut en fait introduire plusieurs topologie sur les domaines (Topologie de Scott, de Lawson) qui redonnent les topologies usuelles (par exemple sur $\mathbb{R}$ ou sur les compacts de $\mathbb{R}$). Classiquement, on définit la calculabilité sur un domaine en ne regardant que la topologie de Scott qui ne donne qu'une notion faible de calculabilité sur les réels. Mais il s'avère qu'en donnant à l'espace une autre topologie, plus fine, on peut retrouver une notion plus *naturelle* ; de plus, ce changement pourrait permettre d'unifier différentes notions de fonctionnelles calculables (bref, le but est de démontrer que la structure topologique de l'espace donne la "calculabilité").

Toutefois, lorsqu'on essaye de parler de calculabilité sur des transformations d'ordre supérieur (fonctionnelles, fonctions sur des fonctionnelles, e.g l'integrale, la mésure), on se rend compte que les espaces topologiques ne sont plus suffisament généraux pour décrire la géométrie de ces espaces. On est amené à introduire les *espaces filtrés* qui en sont une généralisation (ils se basent sur une notion généralisée de "limite"). Dans leur version effective,

ils nous permettraient de définir une notion de calculabilité pour certains morphismes, démontrablement non-topologisable.

Sciences Cognitives

La perspective de travail sur ce thème peut se resumer en deux aspects duaux :

1) L'élargissemant de nos méthodes de preuve (automatiques, en particulier) ;

2) L'analyse mathématique (géométrique) de certains aspects de la cognition humaine (vision, en particulier).

1) Cette partie du projet vise à l'analyse *cognitive* de la "constitution" des objets et des structures mathématiques, qui sont soujacents à la pratique de la preuve et vont au-dela des formalismes logiques. Notre thèse est que certaines structures mathématiques ont un corrélat préconceptuel qui va aussi loin que la structure fine, géométrique, du cerveau (voir 2).

Or, en mathématiques on ne fait pas seulement des preuves, mais on propose ou on construit aussi des concepts et des structures. De plus, le raisonnement (et la déduction mathématique) eux mêmes ne sont pas seulement constitués par "la manipulation de suites discrètes de symboles" (voir l'analyse des incomplétudes modernes dans [10]), mais ils se basent aussi sur des "jugements spatiaux (et temporels)", aussi fondamentaux que les "jugements logiques". Jusqu'à présent, l'analyse des fondements des mathématiques (et, donc, des calculs déductifs) a été essentiellemnt basée sur ces derniers ; notre projet vise à expliciter les principes constitutifs de l'intelligibilité de l'espace (les jugement spatiaux), qui "sont derrière" et permettent la construction des concepts et des structures mathématiques (citons, entr'autres, la connectivité et les symétries : on raisonne, on construit, on démontre - et les physiciens le font depuis longtemps - par symétrie, par exemple).

On pense en fait que l'élargissement des notions de "rigoureux et effectif" aux "vraies" pratiques des mathématiques, grâce à l'analyse des procédures déductives pas nécessairement "linguistico-formels" (mais aussi infinitaires et géométriques), n'est pas seulement un problème épistémologique, mais devrait à terme donner lieu aussi à un enrichissement de nos outils conceptuels et informatiques d'aide à la preuve et au raisonnement.

Le versant technique consistera d'abord dans l'analyse et le développement des démonstrations non-accessibles aux méthodes formelles finitaires (donc non-mécanisable) et telle qu'elles ont étudiées en Théorie de la Démonstration aujourd'hui (voir [29]). Ces démonstrations se basent justement sur des structures d'ordre (arbres, bon-ordre ...) dont la signification est éminemment spatiale. Ensuite la question sera posée des fondements cognitifs de ces invariants conceptuels (parmi lesquels les "jugements spatiaux") que nous proposons pour capturer certaines réguralitеés de l'espace (connectivité, isotropie, symétries, ordre ...).

2) Ce deuxième volé du projet consiste dans l'analyse de la "structuration géométrique" de l'information. En bref, nous pensons que le conténu informationel n'est pas indépendant de la structure géométrique qui code l'information. Dans le cadre du projet "Géométrie et Cognition" (voir dessous), un prémier objectif de ce travail est constitué par l'analyse de la structure fonctionelle du cortex visuelle primaire et de sa géométrie, en tant que lieu d'élaboration de l'information (en collaboration avec J. Petitot, directeur du CREA. et B. Teissier, CNRS-Maths, Paris VII).

Les étonnants développements des neurosciences de la perception permettent, en fait, de commencer à modéliser mathématiquement les mécanismes neuronaux de la perception, la vision en particulier. Un aspect essentiel de cette problématique concerne les liens mathématiques entre l'analyse du signal sensoriel et la structuration géométrique des représentations perceptives. Ce qui nous interesse est la partie géométrique (morphologique) du traitement. En fait, on commence à connaître assez bien l'implémentation des algorithmes permettant au cortex de "faire de la géométrie". On peut juste évoquer ici le champ d'association dans les hypercolonnes d'orientation de l'aire V1 du cortex visuel primaire, champ qui implémente la structure de contact du fibré des directions en chaque point de la rétine. Des champs de tels profils récepteurs agissent par convolution sur le signal et cela à plusieurs échelles différentes. Il serait alors possible de construire à partir d'eux des invariants qui sont des détecteurs de traits géométriques locaux multi-échelle (par exemple des détecteurs de bords, de coins, de points d'inflexion, etc.).

En bref, certains des progrès les plus intéressants dans la compréhension des algorithmes perceptifs concernent la façon dont un traitement du signal peut conduire à une structuration morphologique, c'est-à-dire à une organisation en formes (en patterns). Ces progrès concernent principalement la vision de bas niveau, mais ils comblent un fossé qui jusqu'ici empêchait d'articuler les bas niveaux perceptifs de traitement du signal avec les hauts niveaux plus cognitifs, symboliques et inférentiels. En effet, nous croyons qu'ils expliquent comment se constitue le niveau morphologique des patterns sur lequel se fondent les niveaux cognitifs supérieurs.

Le financement, par le MENRST, du projet interdisciplinnaire "Géométrie et Cognition", dont un membre de l'équipe est le responsable, est le support principal de ces activités (voir dessous et
http ://www.dmi.ens.fr/users/longo/geocogni.html).

Éléments d'évaluation

1 Collaborations

- **Contrats** :
  - Programme Télécommunications du CNRS
    Programmation répartie, collaborative et sécurisée pour Internet.
    Projet commun Équipe LTL (ENS, Paris) et Équipe OASIS (INRIA, Sophia-Antipolis). Responsable G. Castagna. (Dotation : 250Kf pour les trois ans)
    Début : novembre 1999. Fin : janvier 2002.
  - Action intégrée de coopération scientifique et technique franco-italienne, ENS - Université de Vénise
    Techniques d'analyse statique pour la sécurité de la mobilité sur Internet.
    Sous la tutelle des ministères des affaires étrangères et ceux de l'éducation nationale, de la recherche et de la technologie. Responsable français G. Castagna (responsable italien Michele Bugliesi). (Dotation : 44Kf pour l'année)
    Début : janvier 2001. Fin : décembre 2001.
  - Action intégrée de coopération scientifique et technique franco-italienne ENS - Université de Turin.
    Sureté de la mobilité sur Internet : une approche à objets.
    Sous la tutelle des ministères des affaires étrangères et ceux de l'éducation nationale, de la recherche et de la technologie. Responsable français G. Castagna (responsable italien Mariangiola Dezani). (Dotation : 28.5Kf par an pour les deux ans)
    Début : janvier 1999. Fin : décembre 2000.
  - Action bilatérale Académie des Sciences Polonaise/Ambassade de France : contrat d'échange de chercheurs.
    Années 1995-1997
  - European community research training project
    European institute in the logical Foundations of Computer Science (EUROFOCS). Début : janvier 1993. Fin : décembre 1997.
  - NATO (International Scientific Exchange Programme)

Extended Rewriting and Types.
Participants : chercheurs des universités de Londres (Imperial College), Turin, Amsterdam, Oregon, et ENS.
Début : 1997. Fin : 2000.

- Projet TMR
Linear Logic in Computer Science.
Participants : Paris, Marseille, Bologna, Rome, Edimbourg, Oxford, Lisbonne.
Début : 1998. Fin : 2002.
- Contrat CNRS/NSF
Logic based specification and verification tools for concurrent languages.
Participants : ENS, INRIA, École Polytechnique, et Université de Pennsylvanie.
Début : 1999. Fin : 2002.
- Projet ECOS-SUD de coopération avec l'Uruguay
Spécifications et programmes : modèles de calcul, types et implantations.
Responsables : M. Fernández et G. Longo. Participants : ENS, École Polytechnique et Université de la République (Uruguay).
Début : 2000. Fin : 2003.
- Capital Humain et Mobilité (CHM) : G. Longo responsable pour ENS-INRIA-PARIS VII du projet "TYPES" (J.Y. Girard, Marseille, responsable européen).
Début : 1993. Fin : 1998
- INTAS : contrat CE/Russie.
Début : 1995. Fin : 1998.
- Capital Humain et Mobilité, CE : G. Longo responsable pour la region parisienne du Reseau Européen pour le recherche fondamentale en Informatique (EUROFOCS), avec centre principal à Edinburg (G. Plotkin).
Début : 1993. Fin : 1997.
- European community research training project :*European institute in the logical Foundations of Computer Science* (EUROFOCS-training).
Début : 1993. Fin : 1997.

- **Groupes de travail européens ou nationaux** :
  - Esprit Working Group 21836 : *Concurrency and Functions : Evaluation and Reduction* (CONFER 2). [1997-2000]
  - Action Cognitique du MENRST : G. Longo responsable de l'atelier interdisciplinaire "Géométrie et Cognition : le problème mathématique de l'espace physique et du vivant" (14 partécipants : chercheurs en maths., biologie, physique et philosophie). 300 KF sur trois ans. [2000-2002].

- Groupe De Recherche *Algorithmique, Langage et Programmation* (GDR ALP du CNRS). G. Castagna est responsable du groupe "Spécification, vérification, sémantique", pôle *Objets et composants logiciels*. [1999]
- Esprit Working Group 26142 : *Applied Semantics* (APPSEM). [1998-2001]
- Esprit Working Group 21900 : *Types for Proofs and Programs* (TYPES). [1993-1998]
- Groupe De Recherche *Programmation* (GDR 690 du CNRS). [1991-1997]
- Groupe de travail GDR-PRC AMI et ALP *Mélanges de systèmes de réécriture et de systèmes logiques*. Responsables : M. Fernández, R. Di Cosmo, D. Kesner. Depuis 1996.

2 Missions, conférences et séminaires

- Giuseppe Castagna : [2000 :] (16-21 décembre) visite pour collaboration et pour présentation d'un séminaire au département d'Informatique de l'Université de Turin (Italie). (26 octobre-6 novembre et 31 mai-5 juin) :invité pour collaboration et pour donner un cours au Département d'Informatique de l'Université Ca' Foscari de Venise (Italie).(13-20 mai) invité pour donner un cours au Département d'informatique de l'Université Polytechnique de Catalogne, Barcelonne (Espagne). (11-12 janvier) séminaire au Computer Science Departement, Boston University. [1999 :] (11-20 décembre) visite pour présentation d'un séminaire au département d'Informatique de l'Université de Turin (Italie). (4-18 juillet) invité pour collaboration et pour présenter un séminaire à l'Université Ca' Foscari de Venise (Italie). [1998 :] (12-22 décembre) invité pour donner un cours à l'Université d'Udine (Italie) (22-25 novembre) : invité par l'INRIA de Sophia-Antipolis.[1997 :] (9-12 octobre) invité pour présenter un séminaire au Computer Science Department, Carnegie Mellon University, Pittsburgh, Pennsylvania. (10-14 septembre) invité pour présenter un séminaire au Centre Universitaire Informatique de l'Université de Génève, Suisse. (12-14 mars) invité pour présenter un séminaire au LIRMM, Université de Montpellier.

- Maribel Fernández : séminaires à Edimbourg (Grande Bretagne – avril 1998), Montevideo (Uruguay – mai 1998), Braga (Portugal – septembre 1999), Londres (Grande Bretagne – fevrier 2000), Montevideo (Uruguay – avril 2000), La Plata (Argentine – avril 2000), Besançon (France – juin 2000) ; conférences à Punta del Este (Uruguay – avril 2000), Madrid (Espagne – septembre 1999), Paris (France – septembre 1999), Indianapolis (États Unis – juillet 1998), Southampton (Grande Bretagne

–septembre 1997).

– G. Longo :
CONFÉRENCES INVITÉES À DES COLLOQUES 1998 - 2001 :
Conference on "Operations, Sets and Types". Invited lecture : "Vicious circles : in Logic and in Mathematics", Castiglioncello (It.), 3-6 Octobre, 1998.
Symposium on "Foundations in Mathematical and Natural Sciences". Invited lecture : "The 'other way round' : from Biology to Mathematics", Pontificia Universitas Lateranensis, Vatican City, November 26-27, 1998.
Workshop on "Methodology in Cognitive Sciences", lecture on "Mathematical invariance and coding-dependence in Logic and Computer Science, an issue in knowledge representation", Fondation des Treilles, Nice, 7 - 13 Decembre, 1998.
Primo Incontro Annuale del Progetto Cofinanziato "Tecniche formali per la specifica, l'analisi, la verifica, la sintesi e la trasformazione di sistemi software". Conferenziere straniero invitato : "Circolarita' ed equazioni, invarianza e geometria, dalla Teoria dei Tipi ad altri aspetti dell'Informatica", Roma, 21 - 23 Dicembre 1998.
Colloque "L'existence en Mathématiques". Conférence invitée : "Existence, coherence et constructions mathématiques possibles", Paris, 27 Mars 1999.
Workshop on Proof-checking, Japan (Computer Sci. Dept., University of Kyoto), 15 May 1999.
Colloque "Le réel en Mathématiques". Conférence invitée : "Objectivité et construction en Mathématiques", Cérisy, 3 - 10 Septembre 1999.
The *1999 meeting of the British Logic Colloquium*. Invited lecture : "Prototype Proofs and Genericity in Type Theories", Swansea, Wales, September 23-25, 1999.
Colloque "Le rationnalisme : science et philosophie en France et en Italie", Istituto Italiano per gli Studi Filosofici, Napoli : "Il costituirsi del "piano fenomenale" in Matematica, con la Matematica", 10 - 11 Dicembre, 1999.
Colloque "Language and Cognition", Roma (Universita' di Roma II) : "Is Language the only ground for Mathematical Knowledge ?", 18 - 20 Maggio, 2000.
Colloque "Mathématiques 2000 : Mathématiques, calcul, ordinateurs", Paris (ENS) : "The Difference between Diderot's clocks, Turing machines and concurrent systems", 24 mai, 2000.
Colloque "Conoscenza e cognizione", Firenze (It.) : "Sulla natura della logica", 7 Novembre, 2000.
Colloque "Geometria, intuizione ed esperienza", Castiglioncello (It.) :

"Concetti matematici ed oggetti della fisica", 1 e 2 Dicembre, 2000.

Journées d'épistémologie (physique, logique, mathématiques), I H P, Paris : "Principes de preuve et principes de construction : la notion de preuve, en mathématiques, est-elle recursive ?", 5 et 6 Décembre, 2000.

Annual Conference TYPES'2000. Key-Note Lecture : "Formal unprovability of provable properties of numbers and prototype proofs in Type Theory", Durham, UK, December 8 - 12, 2000.

Colloque Mathematics and Cognition, University of Rome II : "Mathematics, intentionality and meaning", February 9 and 10, 2001.

Colloque Logic of Husserl, (Archives Husserl, ENS, Paris) : "De la "généalogie des concepts" (Riemann) à la "élucidation épistémologique" (Husserl) pour les fondements des mathématiques, aujourd'hui", April 27 - 28, 2001.

Colloque en honneur de Gilles Chatelet, Paris, "La métaphore et le geste dans la preuve : relire l'incomplétude mathématique des formalismes avec Gilles Châtelet, au-dela de la Gðdélite", 27-29 June, 2001.

AMS/SMF Meeting (American Mathematical Society and Societé Mathématique de France), Lyon : "Foundations of mathematics : some challenges in the interaction with other sciences", July 17-20, 2001.

Colloque international "Géométrie au vingtième siècle : 1930-2000", Institut Henri Poincaré, Paris : "Les fondements géométriques du calcul et de la logique ; les fondements cognitifs de la géométrie", 24 - 29 septembre 2001.

Colloque international "The Mathematics of Ennio De Giorgi", Scuola Normale Superiore, Pisa : "Concepts and conjectures vs axioms and proofs : reflections and results on and from De Giorgi's foundational approach". October 24 - 27, 2001.

G. Longo : SEMINAIRES ET EXPOSES : Instituto Superior Tecnico, Lisboa, Portugal (Dep. de Matematica ; hôte : A. Sernadas, Janvier 1998). Universita' di Bologna (Dip. di Informatica ; hôte : A. Asperti, 20 Febbraio, 1998). Collège de France, Paris (LPPA ; hôte : A. Berthoz, 24 Mars, 1998). Laboratoire des Maths Discrètes, CNRS, Marseille (Colloque HCM "Types" ; coordinateur : I.Y. Girard, 10 Avril, 1998). Universita di Roma I, Roma (Informatica, Scienze ; hôte : C. Boehm, 21 Aprile, 1998). Universita' di Roma II, Roma (Dip. di Filosofia : hôte : A. Carsetti, 21 Maggio 1998). Brandeis University, Boston (Department of Computer Science ; hôte : H. Mairson, June 25, 1998). Universita' di Pisa, Pisa (Dip. di Informatica ; hôte : G. Levi, 26 Ottobre, 1998). Pontificia Universitas Lateranensis, (Centro di Studi Fenomenologici ; hôte : A. Ales Bello, 28 Novembre, 1998). University of Lisbon, Lisboa (Department of Informatics ; hôte : V. Vasconcelos, Jan. 6, 1999). Universita' di Genova, Genova (Dipartimento di Matematica ; hôte : P. Boero, 11 et 12 Mars, 1999). EHESS, Paris, Seminaire "Histoires des Géometries" (hôte : D. Flement, 10 Mai 1999). University of

Keio, Tokyo, Japan (Philosophy Dept., hôte : M. Okada, 18 and 19 May 1999). Tokyo Inst. of Technology, Japan (Computer Sci. Dept, hôte : M. Takahashi, 20 May 1999). Universita' di Bologna, Bologna (Dipartimento di Matematica ed Informatica ; hôte : A. Asperti, 27 Septembre, 1999). Centro di Filososfia della Scienza, Firenze, 5 Novembre, 1999). Universita' di Torino, Torino (Dipartimento di Informatica ; hôte : M. Dezani, 20 Dicembre, 1999). Universita' di Roma III, Roma (Dipartimenti di Filosofia e di Matematica ; hôte : M. Abrusci, 7 Febbraio, 2000). Universita' di Roma I, Roma (Dipartimento di Informatica ; hôte : A. Labella, 7 Marzo, 2000). Collège de France, Paris (Atelier Espace, hôte : M. Denis, 17 Avril, 2000). Imperial College, London (Departement of Computing ; hôte : A. Edalat, May 10, 2000). Université de Paris VII, Paris (Equipe de Logique ; hôte : P. Ressayre, 15 Mai, 2000). Université de Paris VII, Paris (Labo. Preuves, Programmes et Systèmes ; hôte : P.L. Curien, A Bucciarelli, 8 Juin, 2000). INRIA, Roquencourt (Colloquium ; hôte : M. Kern, 16 Janvier, 2001). Universita' di Rome I (Dip. di Filosofia, hôte : C. Cellucci, 15 Febbraio, 2001). Séminaire Heidelberg-Nancy-Strasbourg, Nancy (hôte : P. Nabonnand, 30 Mars, 2001).

3 Accueil de chercheurs

- **Professeurs et directeurs de recherche invités**

  Michele Bugliesi (Universitá Ca' Foscari di Venezia), janvier 2000. (professeur invité ENS)

  Abbas Edalat (Imperial College, London), juin 1998. (professeur invité ENS)

  Martin Escardo (Edinburgh University), Janvier 2000 et Mai 2001. (professeur invité ENS)

  Angus Macintyre (Edinburgh University), Mars 2001. (professeur invité ENS)

- **Post-doctorants**

  S. Egger (Oxford University), 1998-1999.

4 Diffusion de la connaissance

- G. Castagna :
  - Mise en place et organisation du workshop "Proofs for Mobility" (en collaboration avec Davide Sangiorgi), Gênes, avril 2001.
  - Organisateur de la journée "Java Card : sémantique, optimisations et sécurité" ENS, décembre 1999.

- Co-organisateur de la journée "Spécification, vérification, sémantique" du GDR ALP, Villefranche-sur-mer, janvier 1999.
- Tutorial de 6 heures dans *European Conferences on Object-Oriented Programming 1999* (ECOOP '99). Titre : Foundation of Object-Oriented Programming.
- Tutorial de 6 heures dans *European Joint Conferences of Theory and Practice of Software 1999* (CC, ESOP, FASE, FoSSaCS, TACAS). Titre : Foundation of Object-Oriented Programming.
- Tutorial de 6 heures dans *European Joint Conferences of Theory and Practice of Software 1998* (CC, ESOP, FASE, FoSSaCS, TACAS). Titre : Foundation of Object-Oriented Programming.

– G. Longo :
  - ORGANISATION DE COLLOQUE ET SEMINAIRES A L'E.N.S :
    Co-organisateur, Colloque : *Construction d'objectivité : entre intuition et raisonnement*, ENS, Paris, Janvier 1997.

    Co-organisateur, Colloque : *Wittgenstein et les fondements des Mathématiques*, ENS, Paris, Avril 1998.

    Organisateur, Colloque international : *New programs and open problems in the foundation of mathematics and of its applications*, ENS, Paris, November 13-14, 2000.

    Coordination des réunions et exposés interdisciplinaires du Groupe Cogniscience de l'ENS (environ une fois par mois ; voir aussi le "Centre pour les Systèmes Complexes et la Cognition", CenECC), né sous l'impulsion de J.-P. Nadal (Physique), D. Lestel (Psychologie) et G. Longo.

    Co-organisateur du cycle de séminaires hebdomadaires "Philosophie et Mathématiques".
  - EXPOSES A L'E.N.S. :
    "Les Fondements de l'Arithmétique" Journée de l'ELSAP, Jourdan, janvier 1997 ; "Sur les démonstrations des Théorèmes indémonstrables" Séminaire de Philosophie des Mathématiques, mai 1997 ; "L'infini mathémathique, les machines et les méthaphores" Groupe "La Pensée des Sciences", 27 mai 1998 ; "Mathématiques et Cognition : à partir de l'intelligibilité géometrique de l'espace sensible" (avec B. Teissier), 17 février 1999 ; "Mémoire et objectivité en mathématiques" Séminaire de Philosophie des Mathématiques, mars 2000 ; "Expressivité et incomplétude logique" Cours bref, 2 ou 4 heures, dans le cadre de l'Option Intermagistère ENS en *Science Cognitives*, novembre 97 et 99, février et novembre 2000.
  - INFORMATION SCIENTIFIQUE ET VULGARISATION :
    Istituto Italiano di Cultura, Paris, 12 avril 2000.
    Olimpiadi Nazionali di Matematica, Cesenatico, It., 6 mai 2000.

5 Réalisation et diffusion de logiciels, brevets

– G. Castagna a réalisé une extension du compilateur Java 1.02 pour Solaris pour l'implantation de multi-méthodes (en collaboration avec John Boyland, Carnegie Mellon University). 1997.

6 Participations à l'évaluation de la recherche

– G .Castagna :

Membre (nommé) de la section 27 du CNU (depuis 1999).

Membre et assesseur de la commission de spécialistes, section 27, École Normale Supérieure (depuis 1998).

Membre de la commission de spécialistes, section 27, Université Paris 1 (de 1997 à 2000).

Co-chair du Workshop on "Proofs For Mobility", Genova, avril 2001.

Membre du comité de programme de la "European Conference on Object-Oriented Programming", Budapest, juin 2001.

Tutorial co-chair "European Conference on Object-Oriented Programming", Budapest, juin 2001.

Coéditeur du numéro spécial de *Information and Computation* dedié au "Workshop on Foundation of Object-Oriented Languages".

Membre du comité de programme de la conférence "Langages et Modèles à Objets", Nantes, janvier 2001

Tutorial co-chair "European Conference on Object-Oriented Programming", Nice, juin 2000.

Membre du comité de programme du 7ème Workshop on Foundation of Object-Oriented Languages. Boston, janvier 2000.

Membre du comité de programme de la conférence "Langages et Modèles à Objets", Montreal, janvier 2000.

Membre du comité de programme du 5ème workshop *Mobile Objects Security* Lisbonne, juillet 1999.

Membre du comité de lecture du numéro spécial de la revue L'Objet, "Méthodes formelles pour les systèmes à objets", 1999.

Membre du comité de programme de la conférence "Langages et Modèles à Objets", Villefranche-sur-mer, janvier 1999.

Membre du comité de programme du 4ème workshop on *Security and Mobility*. Brussels, juillet 1998.

Membre du comité de programme de la conférence "Langages et Modèles à Objets", Brest, octobre 1997.

Membre du comité de programme du 4ème Workshop on Foundation of Object-Oriented Languages. Paris, Sorbonne, janvier 1997.

Évaluateur pour les revues internationales :Information and Computation, Theoretical Computer Science, Science of Computer Programming, ACM Transactions on Programming Languages and Systems, Theory and Practice of Object-Oriented Systems

Évaluateur pour les conférences internationales : FASE '97, TLCA '97, FASE '98, LICS '98, SOFTSEM '98, LICS '99, ECOOP '99, SAS '99, TLCA '99, STACS '00, ESOP '00, ECOOP '00, ICALP '00, FMOODS '00, OOPSLA '00, POPL '01, FOOL '01, ESOP '01

– M. Fernández

Membre de la commission de spécialistes, section 27, École Normale Supérieure (depuis 1998).

Membre de la commission de spécialistes, section 27, École Normale de Lyon (depuis 2001).

Membre du comité de programme de la conférence internationale "Rewriting Techniques and Applications" RTA'97.

Membre du comité de programme de la conférence internationale "Rewriting Techniques and Applications" RTA'98.

Membre du comité de programme du workshop international "Intersection Types and Related Systems" ITRS'00.

Membre du comité de programme de la seconde Conf. LatinoAméricaine de Programmation Fonctionnelle, Argentine, 1997.

Évaluateur pour les revues internationales : Applicable Algebra in Engineering Communications and Computing, Fundamenta Informatica, Information and Computation, Journal of Functional Programming, Journal of Symbolic Computation, Theoretical Computer Science, entre autres.

Évaluateur pour les conférences internationales ALP, AMAST, FOOL, FOSSACS, FSTTCS, LICS, MFCS, PLILP, PPDP, RTA, STACS.

– G. Longo :

Editor - in - chief, *Mathematical Structures in Computer Science*, Cambridge University Press, à partir de 1990. (Activité de redaction de loin la plus importante).

Editor, *Information and Computation*, à partir de 1982.

Editor, *Informatique Theoretique et Applications* (auparavant : *R.A.I.R.O.*), à partir de 1985.

Editor, *La Nuova Critica* : rivista di Filosofia della Scienza, à partir de 1993.

Editor, *The Journal of Universal Computer Science*, a Springer electronically available journal, à partir de 1994.

Membre, Steering Committee, *Foundation of Objet-Oriented Languages*, Paris, Janvier 1997.

Membre, Organizing Committee, *HCM meeting on Denotational Semantics*, Siena, Mars, 1997.

Membre, Program Committee, *Logical Foundations of Computer Science* (LFCS97), Yaroslavl, Russie, Juillet 1997.

Membre, Program Committee, *Category Theory and Computer Science* (*CT&CS 97*), S. Margherita Ligure, Septembre 1997.

Membre, Program Committee, *13th IEEE conference on Logic in Computer Science*, Indianapolis (In., USA), Juin 1998.

Membre, Program Committee, *Computer Science Logic*, Brno, Czech Republic, Septembre 1998.

Membre, Comité du Programme, *Journées Francophones des Langages Applicatifs, JFLA'98*, Octobre 1998.

Membre, Organizing Committee, *Workshop on Realizability Semantics*, Trento, Italie, June 1999.

Chairman of the Program Committee, *15th IEEE Conference on Logic in Computer Science, LICS'99*, Trento, Italie, Juillet 1999.

Membre, Comité du Programme, *Foundations of Software Science and Computation Structures, FOSSACS'00*, Berlin, D., Mars 2000.

Membre, Organizing Committee of the *IEEE Conference on Logic in Computer Science, LICS*, from 1997 till 2001 (2000 : Santa Barbara, Ca. ; 2001 : Boston).

Membre du Comité Scientifique du Centre Applications et Mathématiques Sociales (CAMS) de l'EHESS, 1997 et 1998.

Membre du conseil de coordination régional des activités en Cogniscience (CogniSeine, présidé par A. Berthoz, Collège de France), 1997 et 1998.

Member, International Panel for the evaluation of Research in Mathematics and Computer Science in Portugal, Ministry of Science and Technology (réunions : Février 1998 et Janvier 1999, Lisboa.)

Membre de la commission de spécialistes, section 27, ENS (depuis 1997).

Expert (lettres de recommandation demandées) pour le recrutement d'enseignants et chercheurs : Stanford Univ., Boston Univ., Carnegie Mellon Univ., Northwestern Univ., Brown Univ., Stevens Technology Inst., Louisiana State Univ., University of Wisconsin at Madison (USA) ; Birmingham Univ., University of Leicester, Durham Univ., Imperial College (GB) ; Univ. of South Australia (AUS) ; EHESS (Paris) ; une dizaine d'Universités italiennes.

Évaluateur pour nombreuses revues et conférences internationales.

7 Encadrement doctoral

Direction de thèses

– G. Castagna

Francesco Zappa Nardelli. *Analyses statiques de calculs distribués* (depuis octobre 2000).

Silvia Crafa. *Mobilité et Securité*(depuis septembre 2000).

Michele Bugliesi. *Approche à objets pour la sûreté de programmes mobiles* (depuis octobre 1998).

Chen Gang. *Sous-typage, conversion de types et élimination de la transitivité*. Décembre 1998. (Thèse a ayant obtenu le prix Shen Donghai comme meilleure thèse franco-chinoise en 1998).

– M. Fernández

L. Khalil, *Réseaux d'interaction et parallélisme*, École Polytechnique, soutenance prévue en 2002.

– G. Longo

Chen Gang (en collab. avec G. Castagna, voir dessus) soutenue en décembre 1998.

G. Santini *Domaines pour la calculabilité*, depuis octobre 1997.

Frédéric DeJaeger *Calculabilité et convergence non-topologique*, depuis octobre 1999.

Participation à d'autres jurys de thèses

– G. Castagna : 1 jury, 2 rapports.
– M. Fernández : 2 jurys.
– G. Longo : 7 jurys, 5 rapports.

Direction de DEA

– G. Castagna

Francesco Zappa Nardelli. "Typage pour le Seal-calcul". DEA Sémantique, Preuves et Programmation. Année 1999-2000.

Valéry Beaujean. "Sécurité et mobilité en ProActive". DEA Sémantique, Preuves et Programmation. Année 1998-1999.

Maude Pasquier. "Gestion statique d'assertions dans les langages objets". DEA Théorie et Ingénierie des Bases de Données. Année 1998-1999.

Amadou Diallo "Spécification formelle d'un système de commerce électronique sur le Web basé sur des agents mobiles". DEA Théorie et Ingénierie des Bases de Données. Année 1998-1999.

– M. Fernández

L. Khalil, *Systèmes de types pour les réseaux d'interaction*. 1999.

F. Blanqui, *Calcul des constructions et réécriture*. 1998.

– G. Longo

P.-S. Graillou, *Aspects cognitifs des preuves visuelles*. DEA Cognition. Année 1998-1999.

G. Halimi (ENS), *Sémantique du polymorphisme*. DEA Cognition. Anné'e 1999-2000.

G. Santini *Domaines et systèmes dynamiques*. DEA Sémantique Preuves Programmation. Année 1996-1997.

C. Truchet (ENS) *Contuinité non-topologique*. DEA Sémantique Preuves Programmation. Année 1997-1998.

S. Vacca *La forme finie du theoreme de Kruskal*. DEA Sémantique Preuves Programmation. Année 1996-1997.

8 Enseignement

Deuxième cycle

– M. Fernández

Travaux dirigés de *Langages formels, calculabilité, complexité et analyse d'algorithmes* au MMFAI (97, 98, 99, 00, 01)

Travaux dirigés de *Logique Informatique* au MMFAI (00, 01)

Travaux dirigés de *Logique* au MMFAI (00-01)

Responsable du Tutorat en Informatique au MMFAI (99-00,00-01)

Jury du concours ENS-Europe à l'ENS (1999, 2000, 2001)

Secrétaire pédagogique du concours d'entrée à l'ENS (CS), 1997 et 1998

Cours, travaux dirigés et travaux pratiques de *Principes d'interprétation de langages* à l'Université de Paris XI (Orsay), 1999 et 2000.

Travaux dirigés de Programmation Fonctionnelle Avancée (SML) à l'École Nationale Supérieure de Techniques Avancées, 1997.

Troisième cycle

– G. Castagna

DEA d'Informatique I3 : information, interaction, intelligence Universités Paris 1, Paris XI. Cours "Sûreté, Intégrité et Sécurité des Données" Années scolaires 2000-2001. (15 heures)

DEA d'Informatique. Université de Nice, Sophia-Antipolis. Cours "Sémantique des langages de programmation". Années scolaires 1998-1999, 1999-2000. (6 heures)

DEA Programmation : sémantique, preuves et langages. Universités Paris VI, Paris VII, Paris XI, ENS, CNAM (c'était "Sémantique, preuves et programmation" jusqu'à 1999). Cours "Sous-typage et langages à objets" (responsable). Années scolaires 1995-2001. (15 heures par an en moyenne).

DEA Théorie et Ingénierie des Bases de Données. Universités Paris I - Paris XI. Module "Langages de Programmation pour Bases de Données". Années scolaires 1993-2000. (12 heures en moyenne).

DEA d'Informatique. Universités Paris XI - Paris XII, ENS Cachan, SUP'ELEC. Cours "Fondements des langages de programmation". Année scolaire 1996-1997. (6 heures).

– M. Fernández

DEA Programmation : Sémantique, Preuves et Langages, Universités Paris VI, Paris VII, Paris XI, ENS, CNAM. Cours "Équivalence opérationnelle dans les langages déclaratifs" 1999 et 2000 (20 heures par an).

DEA Sémantique, Preuves et Programmation Universités Paris VI, Paris VII, Paris XI, ENS, CNAM Cours "Réécriture" 1997 (3 heures).

– G. Longo

DEA Programmation : Sémantique, Preuves et Langages, Universités Paris VI, Paris VII, Paris XI, ENS, CNAM. Cours "Domaines sémantiques", depuis 1995. (10 heures).

DEA Sciences Cognitives, Universités Paris VII, ENS, Ecole Polythécnique. Cours "Espace et langage dans les fondements des Mathématiques et de l'Informatique", depuis 1998. (14 heures).

Ecoles doctorales

– G. Castagna

Dottorato d'Informatica. Universités de Bologne, Padoue et Venise. "Introduzione all'architettura di sicurezza della Java Virtual Machine" (responsable), Venise, 2000 (3 heures) [en Italien].

Doctorat en Informàtica. Universitat Politècnica de Catalunya. "Tipos, subtipos y seguridad en los lenguajes de objetos" (responsable), Barcelona (Espagne), 2000 (12 heures) [en Espagnol].

Scuola Nazionale dei Dottorati di Informatica delle Facolta' di

Scienze. Cours "Linguaggi per basi di dati ad oggetti", Bertinoro (Italie), 1999 (8 heures) [en Italien].

Ecole Jeunes Chercheurs du GDR de Programmation du CNRS. Cours "Types, programmes fonctionnels et orientés objet". Toulouse (1994), Nancy (1995), Bordeaux (1996), Antibes (1997), Lille (1999), Lyon (2000) (6 heures).

Dottorato d'Informatica. Universita' di Udine. Cours "Fondamenti della programmazione orientata ad oggetti" (responsable). Année scolaire 1998-1999 [en Italien]. (12 heures).

Ecole Jeunes Chercheurs en bases de données. Cours "Langages de Requêtes, types". Montpellier 1997 (4 heures).

– G. Longo

III scuola estiva di Logica, AILA-SILFS, 28-30 Septembre, 1999.

Scuola Superiore dell'Universita' di Catania, Catania (10 heures), 3 - 8 Avril, 2000.

9 Prix et distinctions

Giuseppe Longo est membre de l'Académie des Sciences Européenne depuis 1992.

Publications

Livres

[1] G. Castagna. – *Object-Oriented Programming : A Unified Foundation.* – Boston, Birkäuser, 1997, *Progress in Theoretical Computer Science Series.* ISBN 3-7643-3905-5.

Édition d'actes ou d'ouvrages collectifs

[2] G. Castagna et A. Compagnoni (éditeurs). – *Foundation of Object-Oriented Languages.* – Academic Press, 2000, *Special issue of* Information and Computation. A paraître.

[3] M. Dezani, G. Longo et J. Seldin (éditeurs). – *Lambda-calculus and Logic.* – Cambridge University Press, 1999, *Mathematical Structures in Computer Science*, vol. 9, n° 4, pp. 410 – 596. Volume in honour of Roger Hindley.

[4] G. Longo (éditeur). – *On Computer Science.* – The Monist, Journal in Philosophy of Science, jan. 1999, volume 82, 186p. Special issue.

Articles invités

[5] G. Castagna, R. Rousseau et J.-C. Royer. – Fiabilité des langages à objets : le typage est-il suffisant ? *l'Objet*, vol. 4, n° 1, 1998.

[6] G. Longo. – Géométrie, Mouvement et Espace. *Intellectica*, vol. 25, 1997, pp. 195–218. – Article invite', à partir du livre "Le sens du mouvement", par A. Berthoz, Odile-Jacob, 1997.

[7] G. Longo. – Logica e modelli teorici della Biologia. *Sistemi Intelligenti*, n°1, 1997, pp. 150–155.

[8] G. Longo. – Logique et Informatique. *In : Encyclopédie de Philosophie et Histoire des Sciences*, pp. 586–590. – Press Universitaire de France, 1999.

[9] G. Longo. – The Mathematical Continuum, from Intuition to Logic. *Naturalizing Phenomenology : issues in contemporary Phenomenology and Cognitive Science (section on Mathematics and Formal Methods)*, 1999. – Invited Paper, (Petitot et al eds.) Stanford University Press.

[10] G. Longo. – Mathematical intelligence, infinity and machines : beyond the Gödelitis. *Journal of Consciousness Studies*, vol. 6, n° 11-12, 1999. – Invited paper, special issue on Cognition. A preliminary french version of this paper appeared in *Revue de Synthèse*, n. 1 (pp. 111-138), January 1999.

[11] G. Longo. – The Constructed Objectivity of Mathematics. *In : Proposals in Epistemology. On Quantum Mechanics, Mathematics and Cognition.* – 2001. Invited Paper, (M. Mugur-Schacter et al eds.) Reidel-Kluwer, to appear.

[12] G. Longo. – The reasonable effectiveness of Mathematics and its Cognitive roots. *In : New Interactions of Mathematics with Natural Sciences.* – 2001. Invited paper (L. Boi, editor), Springer, to appear.

Articles dans des revues internationales avec comité de lecture

[13] S. Bakel et M. Fernández. – Normalization results for typeable rewrite systems. *Information and Computation*, vol. 133, n° 2, 1997, pp. 73–116.

[14] F. Barbanera, M. Fernández et H. Geuvers. – Modularity of strong normalization in the algebraic-λ-cube. *Journal of Functional Programming*, vol. 6, 1997, pp. 613–660.

[15] G. Castagna. – Unifying overloading and λ-abstractions : $\lambda^{\{\}}$. *Theoretical Computer Science*, vol. 176, n° 1-2, avr. 1997, pp. 337–345. – Note.

[16] G. Castagna et G. Chen. – Dependent types with subtyping and late-bound overloading. *Information and Computation*, 2000. – A paraître.

[17] M. Fernández. – Negation elimination in empty or permutative equational theories. *Journal of Symbolic Computation*, vol. 26, 1998, pp. 97–133.

[18] M. Fernández. – Type assignment and termination of interaction nets. *Mathematical Structures in Computer Science*, 1998. – Special Issue : Selected papers presented at the Conference on Logic and Models of Computation, Marseille, 1996.

[19] M. Fernández et I. Mackie. – Interaction nets and term rewriting systems. *Theoretical Computer Science*, vol. 190, 1998, pp. 3–39. – Special Issue : Selected papers from CAAP'96.

[20] G. Longo. – Prototype Proofs in Type Theory. *Mathematical Logic Quaterly (formely : Zeitscrift f. Math. Logik und Grundlagen der Math.).*, vol. 46, n° 3, 2000.

[21] G. Longo, K. Milsted et S. Soloviev. – Coherence and Transitivity of Subtyping as Entailment. *Journal of Logic and Computation*, vol. 10, n° 4, 2000, pp. 493–526.

Conférences invitées

[22] G. Chen et G. Longo. – Subtyping parametric and dependent types. Longo's Invited Lecture, School on "Type Theory and Term Rewriting", September, 1997, Glasgow. Revised and submitted for publication in April 2000.

[23] G. Longo. – Rigueur mathématique, Logique et Machines. *In : Colloque "Voir, Entendre, Calculer, Raisonner"*, La Villette, Paris, juin 1997. – Actes à paraître.

[24] G. Longo. – The difference between Clocks and Turing Machines. *In : Functional Models of Cognition*, éd. par A. Carsetti. pp. 211–232. – Reidel, 1999. Conférence invitée au Congrès "Models of Cognition and Complexity Theory", Novembre 1994, Roma.

[25] G. Longo. – Mémoire et objectivité en Mathématique. *In : Colloque "Le réel en mathématiques"*, Cérisy, sept. 1999. – Actes à paraître en 2001.

[26] G. Longo. – Principes de construction et principes de preuve : au sujet du théorème de Kruskal-Friedman. *In : Logiche e Metodi di rappresentazione*. pp. 25–46. – La Nuova Critica, 33, 1999. Invited Lecture, Conference on "Mathematical constructions, inductive procedures and semantics", Rome, 1996.

[27] G. Longo. – Cercles vicieux, Mathématiques et formalisations logiques. *Mathématiques, Informatique et Sciences Humaines*, vol. 151, 2000. – Texte revu d'une Conférence invitée, Colloque "Logiques et sciences humaines - nouveaux aspects", Paris, Juin 1997.

[28] G. Longo. – Mathematics and the biological phenomena. *In : Foundations in Mathematical and Natural Sciences*, éd. par B. et al. – 2001. Invited Lecture, Vatican City, November, 1998, actes à paraître.

[29] G. Longo. – On the proofs of some formally unprovable propositions and prototype proofs in type theory. *In : Types'00 at Durham*, éd. par Z. Luo et et al. – Springer, 2001. Invited Lecture at the Annual Types Meeting, Durham (G.B.), December 2000, to appear.

Communications dans des conférences internationales avec comité de lecture

[30] S. Bakel, F. Barbanera et M. Fernández. – Polymorphic intersection type assignment for rewrite systems with abstraction and β-rule. *In : Proceedings TYPES'99*, éd. par T. Coquand, P. Dybjer, B. Nordstrom et J. Smith. *Lecture Notes in Computer Science*. – Springer, 2000.

[31] J. Boyland et G. Castagna. – Parasitic methods : Implementation of multi-methods for Java. *In : OOPSLA '97, 12th ACM SIGPLAN Conference on Object-Oriented Programming Systems, Languages and Applications*, volume 32(10), pp. 66–76. – 1997.

[32] M. Bugliesi et G. Castagna. – Mobile objects. *In : 7th Workshop on Foundation of Object-Oriented Languages*, Boston, 2000. – (actes électroniques).

[33] M. Bugliesi et G. Castagna. – Secure safe ambients and JVM security. *In : IFIP Workshop on Issues in the Theory of Security*, Genève, 2000. – (actes électroniques).

[34] M. Bugliesi et G. Castagna. – Secure safe ambients. *In : Proc. of the 28th ACM Symposium on Principles of Programming Languages*, London, 2001. – ACM Press.

[35] M. Bugliesi, G. Castagna et S. Crafa. – Typed mobile objects. *In : CONCUR 2000 (11th. International Conference on Concurrency Theory)*, Penn State University Parc, 2000. *Lecture Notes in Computer Science*, n°1877, pp. 504–520. – Springer.

[36] G. Castagna et J. Vitek. – Seal : A framework for secure mobile computations. *In : Internet Programming Languages*, éd. par H. Bal, B. Belkhouche et L. Cardelli. *Lecture Notes in Computer Science*, n°1686, pp. 47–77. – Springer, 1999.

[37] A. Compagnoni et M. Fernández. – An object calculus with algebraic rewriting. *In : Programming Languages : Implementations, Logics, and Programs. Proceedings of PLILP'97. Lecture Notes in Computer Science*, n°1292. – Springer, 1997.

[38] M. Fernández et I. Mackie. – Coinductive techniques for operational equivalence of interaction nets. *In : Proceedings of the 13th Annual IEEE Symposium on Logic in Computer Science (LICS'98)*, Indianapolis, Indiana, 1998. – IEEE Computer Society Press.

[39] M. Fernández et I. Mackie. – A calculus for interaction nets. *In : Proceedings of PPDP'99, Paris. Lecture Notes in Computer Science*, n°1702. – Springer, 1999.

[40] M. Fernández et I. Mackie. – Closed reductions for the λ-calculus. *In : Computer Science Logic, Proceedings of CSL'99. Lecture Notes in Computer Science*, n°1683. – Springer, 1999.

[41] M. Fernández et I. Mackie. – A theory of operational equivalence for interaction nets. *In : Proceedings of the 4th Latin American Theoretical Informatics (LATIN'2000)*, Punta del Este, Uruguay, 2000. *Lecture Notes in Computer Science*, n°1776. – Springer.

[42] T. Fruchart et G. Longo. – Carnap's remarks on Impredicative Definitions and the Genericity Theorem. *In : X International Conf. in Logic, Methodology and Philosophy of Science*, éd. par C. et al. pp. 41–56. – Kluwer Academic Publishers, 1999.

[43] L. Khalil. – Polymorphic types for interaction nets. *In : Proceedings of GRATRA'2000, Joint Appligraph and Getgrats Workshop on Graph*

Transformation Systems, éd. par H. Ehrig et G. Taentzer. pp. 257–266. – Technical University of Berlin Report Number 2000–2, March 2000. (actes électroniques).

Communications dans des conférences nationales avec comité de lecture

[44] J. Vitek et G. Castagna. – Mobile computations and hostile hosts. *In : Journées Francophones des Langages Applicatifs*. pp. 113–132. – Editions Hermès, 1999.

Thèses et habilitations

[45] M. Fernández. – *Des modèles de calcul multiparadigmes déclaratifs : Types, modularité, sémantique.* – Habilitation à diriger des recherches, Université de Paris Sud, France, sept. 2000.

[46] C. Gang. – *Sous-typage, conversion de types et élimination de la transitivité.* – Thèse, Paris 7, 1998. Thèse a ayant obtenu le prix Shen Donghai comme meilleure thèse franco-chinoise en 1998.

Rapports de DEA

[47] V. Beaujean. – *Sécurité et mobilité en ProActive.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1999.

[48] F. Blanqui. – *Calcul des constructions et réécriture.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1998.

[49] A. Diallo. – *Spécification formelle d'un système de commerce électronique sur le Web basé sur des agents mobiles.* – DEA Théorie et Ingénierie des Bases de Données, Paris XI, 1999.

[50] P.-S. Grialou. – *Aspects cognitifs des preuves visuelles.* – DEA Sciences Cognititives, Paris VII, 2000.

[51] G. Halimi. – *Sémantique du polymorphisme.* – DEA Logique, Paris VII, 2000.

[52] L. Khalil. – *Un système de types polymorphe pour les réseaux d'interaction.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1999.

[53] M. Pasquier. – *Gestion statique d'assertions dans les langages objets.* – DEA Théorie et Ingénierie des Bases de Données, Paris XI, 1999.

[54] G. Santini. – *Domaines, espace métriques et systèmes dynamiques.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1997.

[55] C. Truchet. – *Continuité et calculabilité non-topologiques.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1998.

[56] S. Vacca. – *La forme finie de Friedman du théorème de Kruskal.* – DEA Sémantique, Preuves et Programmation, Paris VII, 1997.

[57] F. Zappa Nardelli. – *Types for Seal Calculus.* – DEA Programmation : sémantique, preuves et langages, Paris VII, sept. 2000.

Théorie des réseaux et communications

Composition de l'équipe

- Responsable :
  François Baccelli, directeur de recherche INRIA ;
- Autres membres permanents :
  Bartek Błaszczyszyn, chercheur invité ;
  Dohy Hong, chargé de recherche INRIA ;
- Post-doctorants :
  Stefan Haar, TMR Alapedes jusqu'au 01/02/01 ;
  James Martin, TMR Alapedes, jusqu'au 01/11/00 ;
- Doctorants :
  Thomas Bonald, Doctorant, Corps des Télécoms jusqu'au 01/01/99 ;
  Dohy Hong, Doctorant AMX jusqu'au 01/10/00 ;
  Alexandre Proutieres, Doctorant, FT ;
  Florent Tournois, Doctorant, ENS & Corps des Télécoms ;
  Konstantin Tchoumatchenko, Doctorant UNSA jusqu'au 01/01/00.

Thèmes de recherche

1 Remarque préliminaire

Le groupe TREC existe sous la forme d'une action jointe ENS & INRIA-Rocquencourt depuis début 2000. Les personnes de ce groupe étaient auparavant rattachées au projet INRIA Mistral de Sophia Antipolis.

La période couverte dans ce rapport est celle depuis la création de l'action, début 2000.

Ce groupe se concentre sur la modélisation et le contrôle des réseaux de communication. Sa localisation à l'ENS permet le développement d'activités de nature méthodologique, en complément des travaux fondés sur les relations industrielles en cours avec Alcatel et France Télécom.

Du point de vue scientifique, deux axes principaux sont étudiés : la théorie des réseaux au sens *network calculus* d'une part, et la modélisation des réseaux par la géométrie aléatoire d'autre part.

2 Network calculus

Le *network calculus* qui concerne l'analyse et le contrôle des réseaux de communication par des méthodes algébriques.

Par contrôle, nous entendons ici les notions de régulation de flux ATM et surtout de contrôle en boucle fermée du type de TCP, dont l'analyse et l'amélioration sont des défis majeurs pour la communauté réseaux dans les années à venir ([11], [10], [21]).

Les outils mathématiques sont ceux propres aux systèmes dynamiques à événements : semi-anneaux (max,plus) et inf-convolutions ([20], [22], [17]), ainsi que leurs extensions non linéaires ; les principaux outils mathématiques dans ce cadre sont la théorie ergodique, les méthodes de contraction, le calcul des exposants de Lyapunov, la caractérisation des lois limites, les grandes déviations etc. ([3], [4], [23], [5], [17]). Un des axes développés cette année est celui de l'analyse des grands réseaux ([2], [25], [26], [9]).

Les méthodes algébriques en question sont le sujet central du TMR Alapedes dont les partenaires HP Bristol, les universités de Delft, Louvain et Paris, Metalau (INRIA Rocquencourt) et l'Ecole des Ponts et Chaussées.

Les aspects probabilistes sont aussi couverts par le projet INTAS Asymptotics of Stochastic Networks avec l'université de Novosibirsk.

Ce domaine est aussi fortement lié à l'informatique fondamentale (semigroupes, monoïdes de traces, automates) : [29], [14], [8].

3 Réseaux et géométrie aléatoire

La modélisation des réseaux par la géométrie aléatoire. La géométrie aléatoire est un outil ancien dans les sciences des matériaux et la biologie. Les activités dans le domaine des télécommunications, sur lesquelles nous nous concentrons, sont nouvelles et foisonnantes. Ces techniques apportent beaucoup à tout domaine des communications où la composante planaire ou spatiale est présente : réseau d'accès, boucle locale, multipoint, routage ([6]), jeux distribués, architecture hiérarchique, sans fil, etc. On pourra consulter la page web suivante sur ce sujet :
http ://www.dmi.ens.fr/∼mistral/sg/
ainsi que la thèse de K. Tchoumatchenko [19]. Les travaux les plus récents dans cette direction portent sur les processus de couverture, et notamment la couverture CDMA ([1], [7]) :

- Simulation ϵ-parfaite de processus de couverture CDMA fondée sur les grandes déviations
- Simulation conditionnelle parfaite, fondée sur les méthodes de couplage arrière. Exemple : simulation de l'environnement d'un point sachant qu'il est couvert par k cellules.
- Développements asymptotiques pour les processus de couverture CDMA.

Cet axe fait l'objet d'une CTI de FT et d'un projet RNRT avec l'ENST et FT R& D.

Éléments d'évaluation

1 Collaborations

- Les aspects probabilistes de l'axe "théorie des réseaux" ont fait l'objet de deux projets INTAS consécutifs *Asymptotics of Stochastic Networks* avec l'université de Novosibirsk. Ces projets se terminent en Avril 2001. Un workshop a été organisé en Août 2000 à Novosibirsk dans le cadre du projet INTAS et de l'Institut Lyapounov (avec S. Foss, A. Borovkov et S. Rybko). S. Foss a séjourné à l'ENS en Avril 2000. Les travaux sur les processus semi-markoviens généralisés (GSMP), en collaboration avec J. Mairesse, ont été prolongés à cette occasion. L'autre axe de recherche exploré cette année concerne les réseaux de Jackson généralisés avec des lois de service sous-exponentielles.
- Les aspects algébriques de l'axe "théorie des réseaux" ont fait l'objet du TMR Alapedes qui se termine début 2001. Les partenaires de ce projet sont HP Bristol, les universités de Delft, Louvain et Paris, Metalau et l'Ecole des Ponts et Chaussées.

  Les travaux actuels se concentrent sur
  - l'analyse des systèmes (max ,plus) linéaires en dimension infinie (travaux de J. Martin) ;
  - l'étude de propriétés logiques sur les réseaux de Petri (travaux de S. Haar) ;
  - le calcul des exposants de Lyapunov dans (max ,plus) ;
  - l'analyse de la stabilité de certaines classes de réseaux de type Jackson (voir [28]).

  Deux post-doctorants ont travaillé à l'ENS dans le cadre de ce projet : J. Martin et S. Haar. Les collaborations en cours sont principalement avec le Liafa (J. Mairesse), le Loria (B. Gaujal) et Metalau (S. Gaubert).
- L'axe géométrie aléatoire et communications est l'objet des collaborations suivantes :
  - *CTI de FT* (en cours)

    Les travaux avec FT se concentrent sur deux types d'applications : l'économie des réseaux qui est importante dans le contexte de la

compétition entre les opérateurs, et l'analyse des protocoles ayant une composante spatiale. Parmi les sujets les plus importants actuellement, on peut citer :
  - L'amélioration du fonctionnement du multipoint dans l'Internet et les réseaux ATM. Les travaux en cours portent sur l'analyse de protocoles du type HCBT ([12]).
  - L'optimisation des réseaux cellulaires. Les travaux en cours portent notamment sur la couverture CDMA ([1]).
- *projet RNRT Georges avec l'ENST et FT R& D* (en cours). Une convention de recherche et coopération entre l'INRIA, l'ENST et France Télécom a démarré en 1999 dans le cadre du RNRT intitulé «Georges». Il s'agit de fédérer l'étude des réseaux de télécommunications par la géométrie stochastique. La première revue de ce projet a eu lieu en Octobre 2000.

- Les travaux sur le contrôle de congestion ont permis une collaboration (en cours) avec Alcatel portant sur l'analyse de l'interaction d'un grand nombre de connexions TCP dans le contexte de réseaux comportant des routeurs avec des caractéristiques variées : WFQ, FIFO, priorités etc.
- La collaboration avec Sprint porte sur l'analyse de mécanismes de contrôle de flux dans le contexte multipoint, et notamment sur l'influence de la taille du groupe multipoint et de la forme de l'arbre multipoint sur le débit. ([11], [10]).
- Le projet INRIA/NSF avec Georgia Tech en est à sa première année. Plusieurs échanges ont eu lieu dans ce cadre : R. Serfozo et H. Ayhan ont séjourné une semaine à l'ENS, et J. Martin deux semaines à Georgia Tech.

2 Missions, conférences et séminaires

F. Baccelli Présentations aux conférences et workshops suivants :
- SSC, Ottawa, Juin 2000 (conférence invitée) ;
- Madison, Conference on Stochastic Networks, Juin 2000 (`http://www.cms.wisc.edu/~stochnet/`) ;
- Réunion ALAPEDES 7/8 Juillet, Hamburg, RFA ;
- 3-ième ECM, Barcelone, Juillet 2000 (conférence invitée) ;
- Workshop INTAS, Novosibirsk, Août 2000 ;
- Workshop on Random Matrices, Queues, and Percolation 11-15 Septembre, Bristol (G.B.) (`http://research.microsoft.com/users/ajg/workshop.html`) ;
- Second workshop on the modelling of flow and congestion control mechanisms, Paris, Septembre 2000 (`http://www.ens.fr/~mistral/tcp2.html`) ;

– Séminaire final COST 257 Würzburg, RFA, Octobre 2000 (conférence invitée)
(`http://nero.informatik.uni-wuerzburg.de/cost/Final/programm/programm.htm`).

Présentations à des séminaires : INRIA Rocquencourt, Alcatel, FT R&D, Université de Lyon, Université du Minnesota.

B. Błaszczyszyn Présentations aux conférences et workshops suivants :
– Workshop Eurandom "Stochastic Geometry and Teletraffic" et "Stochastic Geometry and Spatial Statistics", Eindhoven, Avril 2000 ;
– Revue du projet RNRT Georges, Mars 2000.

S. Haar Présentations aux conférences et workshops suivants :
– Réunion ALAPEDES 7/8 Juillet, Hamburg, RFA
– WODES 21-23 Août, Gand, Belgique
– CS & P 9-11 Octobre, Berlin, RFA

D. Hong Présentations aux conférences et workshops suivants :
– Conférence ACM-Sigcomm 2000, Stockholm, Suède, Sept. 2000 ;
– Workshop on the modeling of flow and congestion control mechanisms, ENS, Sept. 2000.
– *10th INFORMS Applied Probability Conference* (Ulm, Allemagne, Juillet 1999).
– *37th Annual Allerton Conference on Communication, Control and Computing*, USA (septembre 99).
– séminaire Bell-Labs, Lucent Technologies, Murray Hill NJ, USA (octobre 99).

J. Martin Présentations aux conférences et workshops suivants :
– South Eastern Probability Days, Atlanta, Mars 2000 ;
– Stochastic Networks Workshop, Madison, Juin 2000 ;
– Convention ALAPEDES, Hamburg, Juillet 2000 ;
– Statistical Mechanics 2000, Cambridge, Août 2000 ;
– Modern Problems in Applied Probability, Novisibirsk, Août 2000 ;
– Microsoft / Hewlett-Packard Workshop, Bristol, Septembre 2000.

Présentations à des séminaires : Ecole Polytechnique, Paris ; Georgia Tech, Atlanta ; Bell Labs, New Jersey ; Motorola, Chicago ; ENS.

F. Tournois Présentations aux conférences et workshops suivants :
– Conférence à l'École de Mines, Fontainebleau, Mai 2000 ;
– Revue du projet Georges, Issy, Octobre 2000.

3 Accueil de chercheurs

– **Professeurs et directeurs de recherche invités**

J. Walrand (UC Berkeley, USA), Octobre 2000, orateur de la conférence de rentrée 2000 en informatique de l'ENS ;

J. Gunawardena (HP Bristol, UK), Professeur invité à l'ENS en

Février-Mars-Avril 2000 ;

S. Foss (Université de Novosibirsk, Russie), Avril 2000 ;

D. Korshunov (Université de Novosibirsk, Russie), Avril 2000 ;

R. Serfozo (Georgia Tech, USA), Décembre 1999 ;

H. Ayhan (Georgia Tech), USA, Décembre 1999.

– **Post-doc invités**
B. Heidergott (Eurandom, Pays Bas), Octobre 2000 ;

4 Diffusion de la connaissance

– Organisation du workshop Eurandom sur la géométrie stochastique pour les réseaux en collaboration avec V. Schmidt et O. Boxma en Avril 2000
(http ://www.eurandom.tue.nl/teletraffic.htm).
– Organisation par B. Błaszczyszyn et K. Tchoumatchenko (FT) du Groupe de Travail "Géométrie Stochastique et Réseaux".
– Cours de F. Baccelli au Summer Research Institute (ICA, EPFL) sur la géométrie aléatoire et les réseaux sans fils en Juillet 2000.
– Cours de F. Baccelli sur l'utilisation des algèbres (max ,plus) pour le contrôle de flux dans les réseaux au workshop "Stochastic Networks", Juin 2000
(http ://www.cms.wisc.edu/∼stochnet/).
– Organisation du *Workshop on the modeling of flow and congestion control mechanisms* à l'ENS, 4-6 Septembre 2000, avec l'INRIA Sophia, Sprint et FT R&D
(http ://www.ens.fr/ mistral/tcp2).
– Animation du séminaire du projet par D. Hong
(http ://www.dmi.ens.fr/ mistral/seminaire.html).
– F. Baccelli a donné une conférence plénière à INFORMS Applied probability 99 (Université d'Ulm) sur les réseaux stochastiques et une conférence plénière sur la géométrie aléatoire et les réseaux de communication à l'ITC 16 à Edinburgh en juin 99.

5 Réalisation et diffusion de logiciels, brevets

– En collaboration avec Zhen Liu (maintenant à IBM Yorktown), nous avons développé une nouvelle méthode de simulation de l'interaction entre un grand nombre de connexions TCP se partageant le même routeur d'accès. Un prototype a été développé en C. Il permet d'étudier le débit obtenu par chaque connexion (moyenne en temps long du débit, fluctuations du débit instantané) sous des hypothèses réalistes de trafic (HTTP, voix, mail etc.) et avec une description dé-

taillée des routeurs Internet. L'idée principale, qui est décrite dans [11], consiste en une méthode de point fixe fondée sur la simulation détaillée d'une connexion et une représentation simplifiée de l'interaction avec les autres connexions. Un brevet a été déposé sur ce type de simulateur.

– Durant son stage de magistère au Loria [20], Anne Bouillard (ENS) a intégré dans le logiciel ERS, sous la direction de B. Gaujal, les méthodes d'analyse de systèmes temps réel proposées dans [22].

6 Participations à l'évaluation de la recherche

– F. Baccelli est membre des comités de programme de INFOCOM 2000 et INFOCOM 2001 et des comités de lecture des journaux suivants : *QUESTA, Annals of Applied Probability, Markov Chains, Mathematics of Operations Research* et *Journal of Discrete Event Dynamical Systems.* Il est membre du groupe de travail IFIP W.G. 7.3. et membre du comité scientifique du département "Stochastic Networks" du centre Eurandom à Eindhoven. Il était par ailleurs membre du *visiting committee* du CWI à Amsterdam (1999).

7 Encadrement doctoral

Direction de thèses

– F. Baccelli

Emmanuel Lety, *Une architecture de communication pour environnements distribués à grande échelle sur l'Internet* [18]. Thèse UNSA soutenue en décembre 2000.

Dohy Hong, *Exposants de Lyapunov de Réseaux Stochastiques Max-Plus Linéaires*[17]. Thèse Ecole Polytechnique soutenue en mai 2000.

Konstantin Tchoumachenko, *Modélisation de réseaux de communication par la géometrie stochastique*[19]. Thèse UNSA soutenue en décembre 1999.

Thomas Bonald, *Stabilité des systèmes dynamiques à événements discrets. Application et contrôle de flux dans les réseaux de télécommunication*[16], Thèse Ecole Polytechnique soutenue en octobre 1999.

8 Enseignement

Deuxième cycle

– Deux nouveaux cours ont aussi été mis en place en deuxième cycle :

Cours de deuxième année au MMFAI sur l'analyse des performances des systèmes informatiques (F. Baccelli et S. Haar).

Cours de majeure de deuxième année à l'X. Cours sur la simulation et la modélisation des réseaux de communication, commun aux deux majeures de deuxième année : Mathématiques Appliquées et Algèbre, Informatique et Applications (F. Baccelli, B. Gaujal [LORIA], C. Graham [Polytechnique] et J. Mairesse [Liafa]), [27].

Troisième cycle

- DEA Algorithmique : F. Baccelli, S. Gaubert [ENSTA], B. Gaujal [LORIA], A. Jean-Marie [LIRMM] et J. Mairesse [LIAFA] ont mis en place une nouvelle filière sur les réseaux dans le cadre du DEA Algorithmique ; cette filière comporte trois cours sur les aspects algébriques et probabilistes. Ces cours sont aussi proposés aux étudiants du DEA Réseaux.
- DEA Probabilités, Paris 6 : Cours sur les processus ponctuels, la stabilité et les grandes déviations des réseaux (F. Baccelli, J. Mairesse [Liafa] et L. Massoulié [Microsoft]).

Publications

Articles dans des revues internationales avec comité de lecture

[1] F. Baccelli et B. Błaszczyszyn. – On a coverage process ranging from the boolean model to the poisson voronoi tessellation, with applications to wireless communications. *à paraître dans A.A.P.*, 2001. – Rapport INRIA 4019, Octobre 2000.

[2] F. Baccelli, A. Borovkov et J. Mairesse. – Asymptotic results on infinite tandem queueing networks. *PTRF*, n°118(3), 2000, pp. 365–405.

[3] F. Baccelli et D. Hong. – Analytic expansions of (max,+) lyapunov exponents. *Annals of Appl. Prob.* – à paraître.

[4] F. Baccelli et D. Hong. – Analyticity of iterates of random non-expansive maps. *Adv. in Appl.Prob.*, vol. 32(1), 2000, pp. 193–220.

[5] F. Baccelli et D. Mac Donald. – Rare events for stationary proceesses. *Stoch. Proc. and Appl.*, n°89, 2000, pp. 141–173.

[6] F. Baccelli, K. Tchoumatchenko et S. Zuyev. – Markov paths on the poisson delaunay graph. *Adv. in Appl.Prob.*, vol. 32(1), 2000, pp. 1–18.

[7] B. Błaszczyszyn, C. Rau et V. Schmidt. – Bounds for clump size characteristics in the boolean model. *Adv. in Appl.Prob.*, vol. 31, 1999, pp. 910–938.

[8] S. Haar. – Occurrence net logics. *Fundamenta Informaticae*, vol. 43, Août 2000, pp. 105–127.

[9] J. Martin. – Point processes in fast jackson networks. *Ann. Appl. Probab.*, 2000. – à paraître.

Communications dans des conférences internationales avec comité de lecture

[10] F. Baccelli et D. Hong. – Tcp is max-plus linear. *In : Proceedings of ACM-Sigcomm*, Stockhom, Suède, Septembre 2000. – Rapport INRIA 3986, Août 2000.

[11] F. Baccelli, D. Hong et Z. Liu. – Fixed point methods for the simulation of a large number of interacting tcp connections. *In : Proceedings of ITCSS*, Girona, Espagne, Avril 2001.

[12] F. Baccelli, D. Kofman et J. Rougier. – Self organizing hierarchical multicast trees and their optimization. *In : Proceedings of Infocom 99*, New York, USA, 1999. – soumis à IEEE ToN.

[13] A. Chaintreau, F. Baccelli et C. Diot. – Impact of network delay variation on multicast session performance with tcp-like congestion control. *In : Proceedings of Infocom 2001*, Anchorage, USA, Avril 2001. – Rapport INRIA 3987, Septembre 2000.

[14] B. Gaujal et S. Haar. – A limit semantics for timed petri nets. *In : Proceedings WODES*, Gent, Belgique, Août 2000. pp. 219–226. – Kluwer.

Communications dans des conférences nationales avec comité de lecture

[15] S. Haar. – Clusters, confusion and unfoldings. *In : Proceedings du Workshop CS&P*, Humboldt-Universität zu Berlin, 2000, pp. 219–226.

Thèses et habilitations

[16] T. Bonald. – *Stabilité des systèmes dynamiques à événements discrets. Application et contrôle de flux dans les réseaux de télécommunication.* – Thèse, Ecole Polytechnique, octobre 1999.

[17] D. Hong. – *Exposants de Lyapunov de Réseaux Stochastiques Max-Plus Linéaires.* – Thèse, Ecole Polytechnique, Mai 2000.

[18] E. Lety. – *Une architecture de communication pour environnements distribués à grande échelle sur l'Internet.* – Thèse, UNSA, décembre 2000.

[19] K. Tchoumatchenko. – *Modélisation de réseaux de communication par la géometrie stochastique.* – Thèse, université de Nice Sophia Antipolis, Décembre 1999.

Rapports de DEA

[20] A. Bouillard. – *Calcul du temps de réponse de systèmes temps réel dans le semi-anneau (max,plus).* – Rapport de stage, Ecole Normale Supérieure, Septembre 2000.

[21] J. Guyon. – *Analyse du protocole de contrôle de flux de l'Internet : cas d'une double connexion.* – Rapport de stage d'option, Ecole Polytechnique, Juin 2000.

Rapports de recherche

[22] F. Baccelli, B. Gaujal et D. Simon. – *Analysis of Preemptive Periodic Real Time Systems using the (max,plus) Algebra.* – Rapport technique n° 3778, INRIA, 1999. soumis à **IEEE CST**, 2000.

[23] S. Gaubert et D. Hong. – *Series Expansions of Lyapunov Exponents and Forgetful Monoids.* – RR n° 3971, Rocquencourt, INRIA, Juillet 2000.

[24] S. Haar. – *On Cyclic Orders and Synchronization Graphs.* – RR n° 4007, Rocquencourt, INRIA, Octobre 2000.

[25] J. Martin. – *Large Tandem Queueing Networks with Blocking.* – RR n° 4036, Rocquencourt, INRIA, Octobre 2000. soumis à *QUESTA.*

[26] J. Martin. – *Linear Growth for Greedy Lattice Animals.* – RR n° 4035, Rocquencourt, INRIA, Octobre 2000. soumis à *Stoch. Proc. Appl.*

Notes de cours

[27] F. Baccelli et P. Brémaud. – *Modélisation et Simulation des Réseaux de Communication.* – Ecole Polytechnique, 2000.

Articles soumis ou en préparation

[28] F. Baccelli et D. Hong. – Slotted jackson networks. – 2000. Soumis à QUESTA.

[29] S. Haar, L. Kaiser, F. Simonot-Lion et J. Toussaint. – Using and translating equivalent models : Timed state machines and time petri nets. – Soumis à TACAS 2001.