Les laboratoires de la FSMP

Fondation Sciences Mathématiques de Paris

Département d'Informatique de l'ENS

UMR 8548
Ecole Normale Supérieure

Direction et administration

Directeur : Jean Ponce
Directeur adjoint : David Pointcheval
Responsable administrative : Joëlle Isnard (01 44 32 20 34)
Secrétaire enseignement : Isabelle Delais (01 44 32 20 45)
Adresse : Ecole normale supérieure, 45 rue d'Ulm, 75230 Paris Cedex 05
Web: http://www.di.ens.fr/

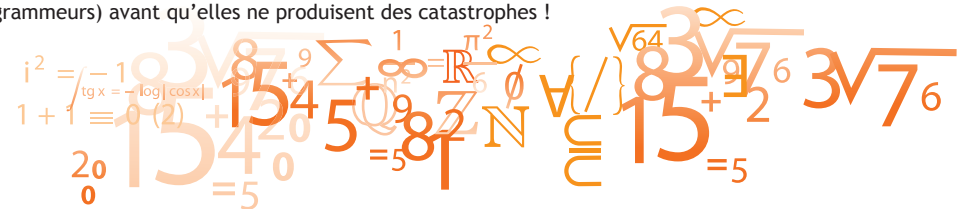
Effectifs et équipes

36 enseignants et chercheurs titulaires
74 chercheurs temporaires (doctorants, post-doctorants et ATER)
Antique Analyse statique par interprétation abstraite - Responsable : Xavier Rival
Cascade Cryptographie - Responsable : David Pointcheval
Data Traitement et classification de signaux - Responsable : Stéphane Mallat
Dyogene Dynamique des réseaux géométriques - Responsable : Marc Lelarge
Parkas Parallélisme des réseaux de Kahn synchrones - Responsable : Marc Pouzet
Security Sécurité informatique - Responsable David Naccache
Sierra Apprentissage statistique - Responsable : Francis Bach
Talgo Théorie, Algorithmes, topoLogie, Graphes et Optimisation - Responsable : Claire Mathieu
Valda Valeur de données - Responsable : Pierre Senellart
Willow Vision artificielle - Responsable : Jean Ponce

Thèmes de recherche

Analyse statique par interprétation abstraite :

- **Sémantique** : En informatique, la sémantique d'un langage fournit pour tout programme écrit dans ce langage un modèle mathématique formel de tous les comportements possibles d'un système informatique exécutant ce programme en interaction avec un environnement quelconque. Toutes les questions intéressantes relatives à la sémantique d'un programme sont indécidables, c'est-à-dire qu'aucun ordinateur ne peut toujours y répondre en un temps fini.
- **Interprétation abstraite** : L'interprétation abstraite est une théorie de l'approximation de sémantiques de langages (de programmation ou de spécification). Elle permet de formaliser l'idée qu'une sémantique est plus ou moins précise selon le niveau d'observation auquel on se place. Si l'approximation est suffisamment grossière, l'abstraction d'une sémantique peut permettre d'en donner une version moins précise mais calculable. La perte d'information ne permet pas de répondre à toutes les questions mais toutes les réponses données par calcul effectif de la sémantique abstraite sont toujours justes. La présentation informelle *Abstract Interpretation in a Nutshell* est une introduction rapide et informelle à la théorie.
- **Analyse statique** : L'analyse statique utilise l'interprétation abstraite pour dériver de la sémantique standard une sémantique 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. Ceci est essentiel, par exemple dans les systèmes informatiques critiques (avions, fusées, centrales nucléaires) pour découvrir les erreurs (qui ont échappé aux programmeurs) avant qu'elles ne produisent des catastrophes !



Cryptographie :

L'activité de recherche de l'équipe Cascade aborde les sujets suivants, qui couvrent presque tous les domaines qui sont actuellement actifs dans la communauté cryptographique internationale:

- *Design and Provable Security in Public-Key Cryptography*
- *Randomness in Cryptography*
- *Lattice Cryptography*
- *Security amidst Concurrency on the Internet*

Traitement et classification de signaux :

- *Invariant Representations with Scattering*
- *Sparse Dictionary and Unsupervised Group Learning*
- *Data Geometry*
- *Inverse problems*

Dynamique des réseaux géométriques :

- *Perfect simulation*
- *Stochastic geometry and information theory*
- *The cavity method for network algorithms*
- *Statistical learning*
- *Network calculus*

Parallélisme des réseaux de Khan synchrones :

Langages de haut niveau formellement définis pour les systèmes embarqués :

- conception, sémantique et mise en œuvre des langages de programmation
- synchrone flot de données concurrence
- répondre à de nouvelles applications : calcul intensif et à grande échelle de simulation, mélange de continu / temps discret

Compilation efficace pour les architectures modernes :

- représentations internes et formellement définies des compilateurs d'optimisation (par exemple, les algorithmes de compilation polyédriques)
- générer du code prouvablement correct et efficace des conceptions synchrones
- cibles modernes processeurs parallèles à mémoire partagée

Apprentissage statistique :

- Apprentissage supervisé
- Apprentissage non supervisé
- Parcimonie
- Optimisation

Théorie, Algorithmes, topologie, Graphes et Optimisation :

Les thèmes de recherche actuels de l'équipe consistent en le développement d'algorithmes et en la découverte de propriétés structurelles pour des problèmes d'origine géométrique et topologique, et pour l'optimisation combinatoire. L'équipe utilise des outils de topologie algébrique, combinatoire, probabilités et optimisation. En termes de communautés, les principaux domaines sont l'algorithmique discrète (SODA) et la géométrie algorithmique (SoCG), avec des liens en combinatoire et théorie des graphes.

Quatre directions de recherche sont actuellement poursuivies :

- l'algorithmique des graphes plongés : algorithmes d'approximation pour les graphes planaires ; algorithmes pour des problèmes topologiques dans les graphes sur les surfaces ;
- algorithmes d'approximation et techniques d'optimisation combinatoire ;
- algorithmes en ligne pour des problèmes de graphes ;
- des problèmes de géométrie combinatoire avec une composante topologique.

Vision artificielle :

- Objet 3D et scène de modélisation, d'analyse et de recherche
- Capture l'activité humaine et de classification
- Catégorie objet de niveau et de reconnaissance de scène
- Apprentissage automatique