UMR 7539

Laboratoire Analyse Géométrie et Application (LAGA)

Direction : **Laurence Halpern**
Ecoles doctorales de rattachement : Cognition, Langage, Interaction ; Université Paris 8 Galilée ; Université Paris 13

Coordonnées :
Université Paris 13, Institut Galilée
99 avenue J.B.Clément
93 430 Villetaneuse
Tel : 01 49 40 38 92
Fax : 01 49 40 35 68
Courriel : laga@math.univ-paris13.fr

Axes de Recherche :
- Géométrie arithmétique, responsable J.Tilouine
- Modélisation et calcul scientifique, responsable F.Weissier
- Physique Mathématiques, responsable A.Grigis
- Probabilités, statistiques, responsable F.Russo
- Théorie ergodique, systèmes dynamiques, responsable P. Le Calvy
- Topologie et théorie des représentations, responsable M.Vigué
- Mathématiques pour le traitement de l'information et de l'image, responsable C. Carlet, F. Dibos

Mots-clés :
Mathématiques discrètes ● Théorie des nombres ● Analyse Numérique ● Equations aux dérivées partielles ● Calcul Scientifique ● Modélisation mathématique et simulation ● Physique mathématique, Probabilités ● Statistiques ● Mathématiques Financières ● Topologie ● Géométrie, Mathématiques divers ● Images ● Traitement du signal ● Protection de l'information ● Systèmes dynamiques

Secteurs d'activité et/ou domaines d'applications :
Voir mots-clés.
Pour l'équipe de Paris 8 : codage d'erreurs, cryptographie.

Partenariats
Agence Nationale de la Recherche (ANR)
Pour Paris 8 :
Projets BOOLE (quantifier des structures booléennes)
Projet BEST (Diffusion Chiffrée pour Télécommunications Sécurisées)

Savoir-faire compétences

Pour l'équipe de Paris 8 :

-Mathématiques pour la protection de l'information
-Codes correcteurs d'erreurs
-Fonctions booléennes pour le chiffrement symétrique
-Cryptographie des cartes à puces
-Partage du secret
-Codes d'authentification
-Courbes elliptiques et cryptographie
-Traçage de traîtres
-Fingerprinting
-Preuves de sécurité

Europe :
(Commission européenne, FSE, autres) Secure Boolean Functions for Coding and Cryptography;
Financement par le Norwegian Research Council
Organismes internationaux

Autres partenaires:
Pôle de compétitivité system@tic, Fonds Unique Interministériel et DGE :
projet SECURE ALGORITHM

Entreprises : THALES OBERTHUR NAGRA Communication & System

Collaborations institutionnalisées :
Nationales : Laboratoire commun avec l'université Paris 13
Internationales : Secure Boolean Functions for Coding and Cryptography
avec l'université de Bergen

Organisation des colloques :
SETA