Application BASTRI
Fiches Equipes

SALSA (SR0096PR)

Résolution de systèmes algébriques et Applications
SPACES (SR0300IR) SALSA (POLSYS (SR0488ZR) , OURAGAN (SR0482BR))

Statut: Terminée

Responsable : Jean-charles Faugère (Par intérim)

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Algorithmique, calcul certifié et cryptographie

Période : 01/11/2005 -> 31/12/2011
Dates d'évaluation : 24/03/2011

Etablissement(s) de rattachement : CNRS, UPMC
Laboratoire(s) partenaire(s) : LIP6 (UMR7606)

CRI : Centre Inria de Paris
Localisation : Antenne Inria Paris-Italie
Code structure Inria : 021039-1

Numéro RNSR : 200518334L
N° de structure Inria: SR0096PR

Présentation

Calcul Formel: Résolution des systèmes polynomiaux, Bases de Gröbner Bases, Complexité, Racines réelles, Système Paramétrés, Géométrie Algorithmique, Calcul symbolique/numérique, Algèbre linéaire haute performance. Cryptologie: Cryptanalyse Algébrique, Attaques par canaux caches, Cryptographie multivariée

Axes de recherche

SALSA est un équipe-projet commune entre l'INRIA, le CNRS et l'Université Pierre et Marie Curie. Notre équipe est reconnue internationalement comme une des équipes particulièrement active dans le domaine de la résolution des équations/inéquations algébriques (systèmes non linéaires) par des méthodes exactes. Notre objectif est de développer des algorithmes efficaces pour calculer les racines complexes, réelles ou dans un corps fini. Les membres de SALSA ont proposé plusieurs algorithmes fondamentaux, en particulier des algorithmes pour le calcul des bases de Gröbner et des algorithmes liés à la méthode des points critiques. Les questions de complexité sont également abordées et récemment l'équipe a obtenu de nouveaux résultats pour les systèmes structurés (systèmes ayant des symétries, systèmes surdéterminés ou bilinéaires, ...) permettant ainsi d'identifier de nouvelles classes de problèmes pouvant être résolues en temps polynomial. L'efficacité pratique de nos algorithmes repose essentiellement sur des librairies d'algèbre linéaire très efficace. Aussi l'équipe est maintenant impliquée dans le développement de librairies d'algèbre linéaire hautes performances. Une forme de validation des algorithmes et des logiciels issus de l'équipe SALSA est de résoudre des défis issus du monde du calcul scientifique. Parmi beaucoup d'autres applications (Robotique, Biologie, Théorie du Signal, ...) le groupe se concentre sur : • Des applications en cryptologie, et en particulier dans le domaine émergent de la Cryptanalyse Algébrique. Le but est d'évaluer la sécurité de cryptosystèmes en se ramenant son étude à la résolution d'un système algébrique à coefficients dans un corps fini. • Des applications en géométrie algorithmique : une nouvelle tendance de ce domaine est de remplacer les objets élémentaires que sont les points et les droites par des courbes. L'intersection de tels objets revient alors à résoudre un système algébrique. • Les problèmes liés au problème de l'optimisation globale qui débouchent eux-mêmes sur d'autres applications en calcul scientifique. Nos logiciels sont systématiquement utilisés pour mener à bien les applications et l'enseignement. La distribution de nos logiciels se fait par l'entremise de la société Maple (WMI Maplesoft Canada) qui intègre dans les distributions récentes l'essentiel des productions logicielles de SALSA. Nous investiguons aussi une nouvelle direction de recherche consistant à certifier symboliquement certains calculs effectués numériquement.

Contact

- **Responsable :** Jean-charles Faugère
- **Tél :** 01.44.27.70.28
- **Secrétariat Tél :** 01.39.63.53.74

En savoir plus

- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité :

Documents sur la structure

- Intranet
- Privés

Décisions

- 4814 (27/01/2006) : création
- 5787 (11/09/2007) : prolongation
- 7531 (28/10/2010) : cessation du responsable
- 7532 (28/10/2010) : nomination responsable
- 7614 (03/01/2011) : prolongation
- 8401 (03/01/2012) : fermeture
- 8337 (19/01/2012) : prolongation

Localisation

- **Adresse postale :** *Non renseignée*
- **Coordonnées GPS :** 48.828738, 2.3509871

Logiciels

- FGb
- Epsilon
- RAGLib

Relations industrielles et internationales

- WMI (Waterloo Maple Inc.)
- CELAR et DGA
- Thalès
- Equipe commune LIAMA Project ECCA (Reliable Software Theme) INRIA/CNRS/UPMC/CAS
- Projet ANR EXACTA (2010-2013) [programme blanc international]
- Réseau d'excellence Européen pour la Cryptologie ECRYPT II (2009-2011)
- Projet Royal Society avec l'équipe Crypto de la Royal Holloway, University of London, UK
- ANR Grant MAC (2007-2010)
- ANR grant CAC (2009-2012) [programme jeunes chercheurs]
- Master Parisien de Recherche en Informatique, Master Paris 6