Application BASTRI
Fiches Equipes

LFANT (SR0415HR)

Théorie algorithmique des nombres rapide et flexible
LFANT (SR0347LR) LFANT CANARI (SR0944PR)

Statut: Terminée

Responsable : Andreas Enge

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : *Aucun mot-clé.*

Domaine : Algorithmique, programmation, logiciels et architectures
Thème : Algorithmique, calcul formel et cryptologie

Période : 01/01/2010 -> 31/08/2023
Dates d'évaluation : 24/03/2011 , 17/03/2015 , 19/03/2019

Etablissement(s) de rattachement : U. DE BORDEAUX, CNRS
Laboratoire(s) partenaire(s) : IMBX (UMR5251)

CRI : Centre Inria de l'université de Bordeaux
Localisation : Institut Mathématiques de Bordeaux (UMR 5251)
Code structure Inria : 091044-1

Numéro RNSR : 201019622P
N° de structure Inria: SR0415HR

Présentation

L'équipe LFANT travaille sur les algorithmes en théorie des nombres et en géométrie arithmétique. Elle couvre toute la chaîne de la conception et l'analyse d'algorithmes passant par des implantations performantes jusqu'aux applications.

Axes de recherche

L'équipe Lfant a pour but de faire l'inventaire des algorithmes majeurs en théorie des nombres, en particulier en théorie algébrique des nombres et en géométrie arithmétique, et d'en proposer des *analyses de complexité*. La plupart de ces algorithmes ont été développés et testés sur des corps de nombres de petit degré and ne passent que difficilement à l'échelle. Des analyses de complexité devraient naturellement mener à des améliorations algorithmiques en identifiant des goulots d'étranglement et en introduisant des approches modernes asymptotiquement rapides.

La *fiabilité* des algorithmes développés est un deuxième objectif à long term de notre équipe. Quitte à démontrer l'hypothèse de Riemann, elle peut être atteinte à travers le déploiement d'algorithmes particuliers, plus lents, qui ne reposeraient sur aucune hypothèse non prouvée. Nous préférerions, par contre, d'ajouter aux algorithmes non prouvés les plus rapides des *certificats* vérifiables indépendamment. Dans l'idéal, il ne devrait pas prendre plus de temps de vérifier ces certificats que de les créer.

Tous nos résultats théoriques sont complémentés par des implantations de référence dans Pari/Gp, permettant ainsi de déterminer et d'ajuster les seuils pour atteindre la complexité asymptotique. Ces implantations aident également à évaluer la performance pratique des algorithmes sur des problèmes de recherche fournis par la communauté. Une autre source de problèmes traités par l'équipe Lfant découle de la cryptologie moderne. Effectivement, la sécurité de tous les cryptosystèmes à clef publique déployés en pratique repose sur la difficulté de résoudre des problèmes en théorie des nombres; inversement, implanter les systèmes et trouver des paramètres sûrs requièrent des algorithmes efficaces.

Logiciels

- PARI/GP
- ARB
- MPC

Contact

- **Responsable :** Andreas Enge
- **Tél :** 05.40.00.61.12
- **Secrétariat Tél :** 05.24.57.41.72

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022

Documents sur la structure

- Intranet
- Privés

Décisions

- 7222 (29/03/2010) : création
- 11315 (14/12/2015) : prolongation
- 14024 (16/12/2019) : prolongation
- 15258 (03/01/2022) : prolongation
- 15503 (01/07/2022) : prolongation

Localisation

- **Adresse postale :** IMB Université de Bordeaux 351, cours de la Libération - F 33 405 Talence France
- **Coordonnées GPS :** 44.4831, 0.3543

- MPFRCX
- CM

Relations industrielles et internationales

Partenaires industriels

- France Télécom R&D
- ST-Ericsson
- Gemalto
- Cryptolog

Collaborations internationales

- University of Calgary
- University of Waterloo
- Universiteit Leiden