Application BASTRI

Fiches Equipes

GRACE (SR0511VR)

Geometry, arithmetic, algorithms, codes and encryption
TANC (SR0144PR) GRACE GRACE (SR0591TR)

Statut: Terminée

Responsable : Daniel Augot

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 certifié et cryptographie

Période : 01/01/2012 -> 30/06/2013
Dates d'évaluation :

Etablissement(s) de rattachement : <sans>
Laboratoire(s) partenaire(s) : <sans UMR>

CRI : Centre Inria de Saclay
Localisation : Centre de recherche Inria de Saclay
Code structure Inria : 111032-1

Numéro RNSR : 201221041Y
N° de structure Inria: SR0511VR

Présentation

La théorie algorithmique des nombres et les problèmes computationnels associés aux courbes algébriques sur les corps, les anneaux, sont centraux dans notre thème de recherche. Ce domaine très riche des mathématiques et de l'informatique a déjà montré son importance dans la cryptographie à clé publique, avec des succès industriels comme le système RSA et la cryptographie à base de courbes elliptiques. Il est moins connu que de bons codes correcteurs d'erreur ou autres peuvent être construits avec les mêmes objets mathématiques, qui sont aussi au coeur de Grace. Nous pensons qu'une interprétation géométique et unifiée donne une vue profonde sur la nature et les performances des ces problèmes en théorie des codes et cryptographie. Ces deux domaines d'applications interviennent pour la fiabilité et la sécurité des applications. Alors que la cryptologie est traditionnellement au cœur de l'informatique, ce n'est que plus récemment que la théorie des codes y trouve des applications, en sortant du document des télécommunications.

Axes de recherche

En utilisant la théorie des nombres et la géométrie sur les coprs finis, Grace vise à construire de meilleurs cryptosystèmes, mieux définir leur sécurité pour déterminer les bonnes tailles de clé, construire les meilleurs codes algébriques.

Relations industrielles et internationales

DTU Lyngby Ulm Universität University of Auckland Alcatel Lucent

Contact

- **Responsable :** Daniel Augot
- **Tél :**
- **Secrétariat Tél :** 01..7.7..57..8.1..31

En savoir plus

- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023 , 2024

Documents sur la structure

- Intranet
- Privés

Décisions

- 8408 (10/01/2012) : création
- 8415 (01/01/2012) : nomination responsable
- 9143 (16/01/2013) : prolongation

Localisation

- **Adresse postale :** Centre de recherche Inria de Saclay Campus de l'École Polytechnique - Bâtiment Alan Turing 1 rue Honoré d'Estienne d'Orves 91120 Palaiseau France
- **Coordonnées GPS :** 48.714, 2.206