# Application BASTRI

## Fiches Equipes

## GRACE (SR0591TR)

Geometry, arithmetic, algorithms, codes and encryption
GRACE (SR0511VR)  GRACE

**Statut:** Décision signée

**Responsable :** Alain Couvreur

**Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" :** A2.3.1. Systèmes embarqués , A4.2. Codes correcteurs , A4.3.1. Cryptographie à clé publique , A4.3.3. Protocoles cryptographiques , A4.4. Sécurité des équipements et des logiciels , A4.6. Authentification , A4.8. Technologies pour la protection de la vie privée , A4.9. Supervision de la sécurité , A7.1. Algorithmique , A8.1. Mathématiques discrètes, combinatoire , A8.4. Calcul formel, calcul algébrique , A8.5. Théorie des nombres

**Mots-clés de "B - Autres sciences et domaines d'application - 2023" :** B5.11. Systèmes quantiques , B6.4. Internet des objets , B6.6. Systèmes embarqués , B9.5.1. Informatique , B9.5.2. Mathématiques , B9.10. Confidentialité, vie privée

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

**Période :** 01/07/2013 -> 31/12/2024
**Dates d'évaluation :** 17/03/2015 , 19/03/2019 ,

**Etablissement(s) de rattachement :** CNRS, IP-PARIS
**Laboratoire(s) partenaire(s) :** LIX (UMR7161)

**CRI :** Centre Inria de Saclay
**Localisation :** Centre de recherche Inria de Saclay
**Code structure Inria :** 111032-2

**Numéro RNSR :** 201221041Y
**N° de structure Inria:** SR0591TR

### 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 domaine des télécommunications.

### Axes de recherche

En utilisant la théorie des nombres et la géométrie sur les corps 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 :** Alain Couvreur
- **Tél :**
- **Secrétariat Tél :** 01..7.7..57..8.1..31

### En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2015 , 2016 , 2017 , 2018 , 2019 , 2020 , 2021 , 2022 , 2023

### Documents sur la structure

- Intranet
- Privés

### Décisions

- 9566 (10/09/2013) : création
- 11315 (14/12/2015) : prolongation
- 14024 (16/12/2019) : prolongation
- 14652 (18/01/2021) : cessation du responsable
- 14653 (18/01/2021) : nomination responsable
- 16661 (11/12/2023) : prolongation
- 17000 (26/04/2024) : 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