Application BASTRI
Fiches Equipes

CANARI (SR0944PR)

Analyse cryptographique et arithmétique
LFANT (SR0415HR) CANARI

Statut: Décision signée

Responsable : Damien Olivier Robert

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : A4.3.1. Cryptographie à clé publique , A4.3.3. Protocoles cryptographiques , A4.3.4. Cryptographie quantique , A8.5. Théorie des nombres , A8.10. Arithmétique des ordinateurs

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : B9.5.1. Informatique , B9.5.2. Mathématiques , B9.8. Recherche reproductible , B9.10. Confidentialité, vie privée

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

Période : 01/07/2023 -> 30/06/2027
Dates d'évaluation :

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

CRI : Centre Inria de l'université de Bordeaux
Localisation : Institut Mathématiques de Bordeaux (UMR 5251)
Code structure Inria : 091073-0

Numéro RNSR : 202324429H
N° de structure Inria: SR0944PR

Présentation

Le but de l'équipe Canari est de développer des algorithmes efficaces pour traiter les objets du programme de Langlands : formes automorphes, représentations galoisiennes, motifs et fonctions L. En tant que briques de base, nous développons des algorithmes efficaces et rigoureux pour l'arithmétique et l'analyse. Enfin, nous appliquons nos algorithmes à la cryptographie : cryptographie post-quantique, mpc, chiffrement fonctionnel et homomorphe.

Nous mettons fortement l'accent sur le développement de logiciels open source :

- Pari/GP
- Flint, Arb, Calcium
- MPC

Axes de recherche

- Algorithmes pour la théorie des nombres en dimension supérieure
- Analyse efficace
- Cryptographie de nouvelle génération et post-quantique

Relations industrielles et internationales

- DGA
- IBM Zurich

Contact

- **Responsable :** Damien Olivier Robert
- **Tél :** 06.66.56.25.49
- **Secrétariat Tél :** 05.24.57.40.02

En savoir plus

- Site de l'équipe
- Site sur inria.fr
- Site du responsable
- Derniers Rapports d'Activité : 2023

Documents sur la structure

- Intranet
- Privés

Décisions

- 16327 (30/06/2023) : création

Localisation

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