Application BASTRI

Fiches Equipes

CODES (SR0216RR)

Codes et cryptographie
CODES SECRET (SR0097JR)

Statut: Terminée

Responsable : Nicolas Sendrier

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 : Systèmes symboliques
Thème : Structures algébriques et géométriques, algorithmes

Période : 01/01/1986 -> 31/12/2007
Dates d'évaluation :

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

CRI : Centre Inria de Paris
Localisation : Rocquencourt
Code structure Inria :

Numéro RNSR : 198621349W
N° de structure Inria: SR0216RR

Présentation

La recherche au projet CODES se consacre à la construction et à l'analyse d'algorithmes cryptographiques à travers l'étude des structures discrètes que ceux-ci induisent.
Excellence : cryptographie symétrique, mathématiques discrètes, algorithmique.

Domaines de compétence : nos compétences en mathématiques et algorithmique (corps finis, combinatoire, théorie de l'information) nous permettent de traiter un large spectre de problème liés à la protection de l'information. La plupart de nos travaux mélangent des aspects fondamentaux (étude d'objets mathématiques), et les aspects pratiques (cryptanalyse, conception d'algorithmes, implémentation).

Domaines d'application : nos domaines d'applications sont principalement la cryptologie, les codes correcteurs d'erreur, et la reconnaissance de code ("guerre électronique"). Bien que ces domaines puissent apparaitre assez différents, notre approche est unifiée. Par exemple, les techniques de décodage sont utilisées pour concevoir de nouveaux codes correcteurs d'erreur, mais aussi de nouvelles cryptanalyses. La reconnaissance de codes (c'est-à-d-ire reconnaître un schéma de codage inconnu à partir d'un train binaire), est très semblable à la cryptanalyse des chiffrements à flots.

Axes de recherche

Analyse de la sécurité des algorithmes cryptographiques symétriques : chiffrement par bloc (AES), chiffrement par flot ECRYPT
Codage et cryptographie: alternatives à RSA, systèmes résistant à l'ordinateur quantique.

Algorithmes de décodage et applications: bloc turbo-codes, correction de forts taux d'erreur.

Reconnaissance de codes : guerre électronique.

Relations industrielles et internationales

- Université de Limoges
- Université de Bergen
- France Télécom R & D
- CELAR

Contact

- **Responsable :** Nicolas Sendrier
- **Tél :** 01.39.63.52.47
- **Secrétariat Tél :** 01.39.63.52.62

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 3730 (09/12/2002) : modification
- 4530 (22/02/2005) : prolongation
- 5787 (11/09/2007) : prolongation
- 5994 (30/01/2008) : fermeture

Localisation

- **Adresse postale :** *Non renseignée*
- **Coordonnées GPS :** 48.83703, 2.103342