Application BASTRI
Fiches Equipes

SECRET (SR0097JR)

Sécurité, Cryptologie et Transmissions
CODES (SR0216RR) □ SECRET □ COSMIQ (SR0886CR)

Statut: Terminée

Responsable : Anne Canteaut

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : *Aucun mot-clé.*

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : *Aucun mot-clé.*

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

Période : 01/07/2008 -> 30/11/2019
Dates d'évaluation : 24/03/2011 , 17/03/2015 , 19/03/2019

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

CRI : Centre Inria de Paris
Localisation : Centre de recherche Inria de Paris
Code structure Inria : 021088-1

Numéro RNSR : 200818335Z
N° de structure Inria: SR0097JR

Présentation

Les travaux de recherche de l'équipe-projet SECRET sont essentiellement consacrés à la conception et à l'analyse de la sécurité d'algorithmes cryptographiques, dans le contexte classique ou quantique.

Ils sont notamment motivés par le fait que la cryptographie est actuellement dans une situation relativement fragile : la sécurité des primitives disponibles, symétriques ou asymétriques, est en effet menacée par les progrès récents de la cryptanalyse ou par l'éventuelle construction d'un ordinateur quantique. La plupart de nos travaux combinent les aspects fondamentaux et pratiques de la protection de l'information (cryptanalyse, conception d'algorithmes, mise en oeuvre).

Axes de recherche

- **Cryptographie symétrique :** Nos travaux portent à la fois sur les chiffrements à flot, par blocs et les fonctions de hachage. Ils abordent conjointement tous les aspects de la cryptographie symétrique, des aspects les plus pratiques (attaques effectives de systèmes existants, conception de nouveaux chiffrements) aux plus théoriques, fondés sur les mathématiques discrètes.
- **Cryptographie fondée sur les codes :** Les primitives cryptographiques exploitant des problèmes difficiles émanant de la théorie des codes offrent une alternative crédible aux algorithmes qui reposent sur des problèmes issus de la théorie des nombres. On les qualifie souvent de post-quantiques dans la mesure où, contrairement au RSA, leur sécurité n'est pas remise en cause par l'apparition de la machine quantique. Nos travaux portent sur l'analyse de la sécurité de ce type de systèmes, leur mise en oeuvre pratique et également sur la conception de primitives efficaces fondées sur les codes.
- **Rétro-ingénierie des systèmes de communication :** Quand on intercepte une communication non chiffrée mais bruitée, on ne peut accéder à l'information transmise que si on a au préalable retrouvé les spécifications des éléments constitutifs du système de transmission utilisé (brasseur, codeur de canal...). Nous menons des travaux de recherche sur cet aspect de rétro-ingénierie qui portent notamment sur la reconnaissance des brasseurs et des différents codes correcteurs utilisés lors d'une transmission.
- **Théorie de l'information quantique :** L'obstacle principal au développement de l'informatique quantique est la décohérence, qui résulte de l'interaction entre l'ordinateur et l'environnement extérieur. Afin de lutter contre cet effet, nous explorons diverses approches pour

Contact

- **Responsable :** Anne Canteaut
- **Tél :** 01.80.49.42.20
- **Secrétariat Tél :** 01.80.49.40.47

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 6235 (11/07/2008) : création
- 8337 (19/01/2012) : prolongation
- 11315 (14/12/2015) : prolongation
- 14055 (23/12/2019) : fermeture

Localisation

- **Adresse postale :** Centre Inria de Paris 48, rue Barrault CS 61534 75647 PARIS CEDEX
- **Coordonnées GPS :** 48.8263366, 2.3464412

la correction d'erreurs quantiques. Nous étudions plus particulièrement certaines familles de codes correcteurs quantiques qui généralisent les meilleurs codes classiques connus. Nos recherches portent également sur la cryptographie quantique : nous étudions la sécurité de protocoles efficaces de distribution de clefs, en étroite collaboration avec des expérimentateurs. Plus généralement, nous étudions l'impact de la physique quantique sur l'action des différents protagonistes d'un scénario cryptographique.

Relations industrielles et internationales

- ANR : projets BLOC, KISS et CLE
- Délégation Générale pour l'Armement, CELAR
- XLIM, Université de Limoges et CNRS
- Selmer Center, Université de Bergen, Norvège
- DTU Compute, Danish Technical University, Danemark
- Institut f\"ur Algebra und Geometrie, Otto-von-Guericke Universit\"at Magdeburg, Allemagne
- Indian Statistical Institute, Calcutta, Inde
- ITTP, institut de l'académie des sciences russe