Application BASTRI

Fiches Equipes

COSMIQ (SR0886CR)

Cryptologie symétrique, cryptologie fondée sur les codes et information quantique
SECRET (SR0097JR) COSMIQ

Statut: Décision signée

Responsable : Jean-pierre Tillich

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2023" : A1.2.8. Sécurité des réseaux , A3.1.5. Contrôle d'accès, confidentialité , A4. Sécurité et confidentialité , A4.2. Codes correcteurs , A4.3. Cryptographie , A4.3.1. Cryptographie à clé publique , A4.3.2. Cryptographie à clé secrète , A4.3.3. Protocoles cryptographiques , A4.3.4. Cryptographie quantique , A6.2.3. Méthodes probabilistes , A7.1. Algorithmique , A7.1.4. Algorithmique quantique , A8.1. Mathématiques discrètes, combinatoire , A8.6. Théorie de l'information

Mots-clés de "B - Autres sciences et domaines d'application - 2023" : B6.4. Internet des objets , B6.5. Systèmes d'information , 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 : 01/12/2019 -> 31/12/2024
Dates d'évaluation :

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 : 021157-0

Numéro RNSR : 201923488C
N° de structure Inria: SR0886CR

Présentation

Les travaux de recherche de l'équipe-projet**COSMIQ** 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

Algorithmes quantiques et cryptanalyse

Les ordinateurs quantiques ont un impact profond sur la cryptographie. Dans cet axe de recherche nous étudions cet impact

- en concevant de nouvelles attaques quantiques à la fois en cryptographie symétrique et en cryptographie asymétrique en adaptant au cadre quantique des techniques classiques de cryptanalyse
- mais aussi en concevant directement de nouvelles attaques quantiques qui n'ont pas de pendant classique.

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 la difficulté du problème de

Contact

- **Responsable :** Jean-pierre Tillich
- **Tél :** 01. 8.0 .49. 4.2 .22
- **Secrétariat Tél :** 01. 8.0 .49. 4.0 .47

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 13957 (18/11/2019) : création
- 16661 (11/12/2023) : prolongation
- 17000 (26/04/2024) : prolongation

Localisation

- **Adresse postale :** Centre de recherche Inria de Paris 2 rue Simone Iff Voie DQ12 75012 Paris France
- **Coordonnées GPS :** 48.84161, 2.38446

décodage d'un code linéaire offrent une alternative crédible à RSA ou à DSA pour obtenir des cryptosystèmes résistant à un ordinateur 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.

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 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
- ANSSI
- Délégation Générale pour l'Armement, CELAR
- Orange Labs Caen
- ATOS
- Thales
- Paris Centre for Quantum Computing
- XLIM, Université de Limoges et CNRS
- Université de Bordeaux
- Université de Rennes
- Université de Rouen
- Université de Versailles

- NTT, Japon
- Université de Bochum, Allemagne
- Université de Nagoya, Japon
- Université de Sheffield, Royaume UniTU Delft and TU Munich.
- Université technique de Graz, Autriche
- Université Technologique Nanyang, Singapour
- Université Tsinghua, Pékin, Chine
- TU Delft, Pays Bas
- TU Eindhoven, Pays Bas