Application BASTRI

Fiches Equipes

CAPSULE (SR0935UR)

Cryptographie Appliquée et Sécurité des Implémentations
CAPSULE

Statut: Décision signée

Responsable : Pierre-alain Fouque

Mots-clés de "A - Thèmes de recherche en Sciences du numérique - 2024" : A1.2.8. Sécurité des réseaux , A4.3. Cryptographie , A4.3.1. Cryptographie à clé publique , A4.3.2. Cryptographie à clé secrète , A4.3.3. Protocoles cryptographiques , A4.6. Authentification , A4.8. Technologies pour la protection de la vie privée , A7.1.4. Algorithmique quantique , A8.5. Théorie des nombres

Mots-clés de "B - Autres sciences et domaines d'application - 2024" : B6.4. Internet des objets , 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 : 01/01/2023 -> 31/12/2026
Dates d'évaluation :

Etablissement(s) de rattachement : U. RENNES
Laboratoire(s) partenaire(s) : IRISA (UMR6074)

CRI : Centre Inria de l'Université de Rennes
Localisation : Centre Inria de l'Université de Rennes
Code structure Inria : 031138-0

Numéro RNSR : 202324388N
N° de structure Inria: SR0935UR

Présentation

Les activités de recherche de l'équipe CAPSULE sont organisés autour de 5 axes de recherches, la cryptographie symétrique, la cryptographie post-quantique, la sécurité des implémentations matérielles et logicielles de cryptographie, la cryptanalyse quantique et la cryptographie dans la vie réelle.

Axes de recherche

- La conception et l'analyse de chiffrements: chiffrement par bloc léger, schéma de chiffrement authentifié, etc;
- Cryptographie à base de réseaux euclidiens, preuves de sécurité et constructions avancées, déploiement des normes de chiffrement post-quantique;
- La cryptographie et cryptanalyse quantique;
- Sécurité des implémentations cryptographiques: attaques par canaux auxiliaires, attaques par micro-architecture et contremesures;
- Conception et Analyse de systèmes et protocoles cryptographiques dans la vie réelle comme les messageries sécurisées WhatsApp et Signal ou la sécurité des bases de données avec les schémas de chiffrement symétrique cherchable.

Relations industrielles et internationales

L'équipe Capsule a des relations avec les équipes de cryptographie au CWI (Amsterdam, Pays-Bas), à King's College (Londres, Royaume-Unis), Max Planck Institute for Security and Privacy (Bochum, Allemagne) et des relations industrielles et gouvernementales avec (PQShield SA, NTT, KDDI, Thales, Alice&Bob, Orange Labs, CryptoExperts, Zama, ANSSI, DGA).

Contact

- **Responsable :** Pierre-alain Fouque
- **Tél :** 02..9.9..84..7.5..58
- **Secrétariat Tél :** 02..9.9..84..7.5..00

En savoir plus

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

Documents sur la structure

- Intranet
- Privés

Décisions

- 15889 (03/01/2023) : création
- 16259 (03/07/2023) : modification

Localisation

- **Adresse postale :** Centre Inria de l'Université de Rennes 263, avenue du Général Leclerc Campus universitaire de Beaulieu 35042 Rennes Cedex France
- **Coordonnées GPS :** 48.116, -1.64