Offer #2024-08482

Doctorant F/H Cryptanalyse des modes opératoires en cryptographie symétrique.

The offer description below is in French

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Context

Dans le cadre du projet ciblé CRYPTANALYSE du PEPR Cybersécurtié

L' objectif est de réaliser des recherche pour améliorer la compréhension et les connaissances sur la sécurité des constructions symétriques. Une première partie plus concrète portera sur l'étude de la sécurité de différents modes et constructions à travers de la cryptanalyse.

Assignment

Le sujet de thèse porte sur la cryptanalyse des modes opératoires en cryptographie symétrique.

En particulier, nous souhaitons d'abord étudier le mode f8, utilisé dans la téphonie 3G, avec des attaques génériques dans la lignées de travaux préc'ents sur les modes CTR et CBC:

- https://dx.doi.org/10.1145/2976749.2978423
- https://dx.doi.org/10.1007/978-3-319-78375-8_24

Collaboration :
La thèse sera co-encadrée par María Naya-Plasencia et Gaëtan Leurent

Main activities

Le candidat devra:

- lire des articles scientifiques sur le sujet;
- mener des recherches en collaboration avec ses encadrants;
- rédiger des articles scientifiques;
- présenter ses résultats lors de congrés ou de séminaires.

Benefits package

- Restauration subventionnée
- Transports publics remboursés partiellement
- Congés: 7 semaines de congés annuels + 10 jours de RTT (base temps plein) + possibilité d'autorisations d'absence exceptionnelle (ex : enfants malades, déménagement)
- Possibilité de télétravail (après 6 mois d'ancienneté) et aménagement du temps de travail
- Équipements professionnels à disposition (visioconférence, prêts de matériels informatiques, etc.)
- Prestations sociales, culturelles et sportives (Association de gestion des œuvres sociales d'Inria)
- Accès à la formation professionnelle
- Sécurité sociale

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Paris
- **Starting date :** 2025-02-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-01-16

Contacts

- **Inria Team :** COSMIQ
- **PhD Supervisor :**
  Leurent Gaetan / gaetan.leurent@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.