Offre n°2024-08482

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

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

Contexte et atouts du poste

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.

Mission confiée

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

Principales activités

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.

Avantages

- 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

Informations générales

- **Thème/Domaine :** Algorithmique, calcul formel et cryptologie
- **Ville :** Paris
- **Centre Inria :** Centre Inria de Paris
- **Date de prise de fonction souhaitée :** 2025-02-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2025-01-16

Contacts

- **Equipe Inria :** COSMIQ
- **Directeur de thèse :**
  Leurent Gaetan / gaetan.leurent@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.