Offre n°2025-09151

Chercheur contractuel / Cryptologie

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Chercheur contractuel

A propos du centre ou de la direction fonctionnelle

*Le centre de recherche Inria de Saclay a été créé en 2008. Sa dynamique s'inscrit dans le développement du plateau de Saclay, en partenariat étroit d'une part avec le pôle de l'**Université Paris-Saclay** et d'autre part avec le pôle de l'**Institut Polytechnique de Paris** . Afin de construire une politique de site ambitieuse, le centre Inria de Saclay a signé en 2021 des accords stratégiques avec ces deux partenaires territoriaux privilégiés.*

*Le centre compte **40 équipes-projets**, dont 32 sont communes avec l'Université Paris-Saclay ou l'Institut Polytechnique de Paris. Son action mobilise **plus de 600 personnes**, scientifiques et personnels d'appui à la recherche et à l'innovation, issues de 54 nationalités.*

Le centre Inria Saclay - Île-de-France est un acteur essentiel de la recherche en sciences du numérique sur le plateau de Saclay. Il porte les valeurs et les projets qui font l'originalité d'Inria dans le paysage de la recherche : l'excellence scientifique, le transfert technologique, les partenariats pluridisciplinaires avec des établissements aux compétences complémentaires aux nôtres, afin de maximiser l'impact scientifique, économique et sociétal d'Inria.

Contexte et atouts du poste

Dans le cadre du consortium HYPERFORM (Bpifrance).

L' objectif est de faire de la recherche fondamentale en cryptographie post-quantique, plus particulièrement la cryptologie hybride et agile.

Mission confiée

Missions :
Avec l'aide de Benjamin Smith et autres membres du consortium HYPERFORM,

la personne recrutée sera amenée à faire de la recherche fondamentale en cryptologie post-quantique.

Le projet se porte sur la cryptographie post-quantique, avec un focus special sur les cryptosystèmes basés sur les isogénies. Plus spécifiquement, le candidat travaillera sur la conception et optimisation des algorithmes dans la cryptographie post-quantique qui apportent de la "crypto-agilité" : c'est à dire, on cherche des algorithmes efficaces mais flexibles, qui peuvent être utilisé dans plusieurs cryptosystèmes, ou dans plusieures instances d'un seul cryptosystème (avec des parametres qui évoluent). La crypto-agilité est souhaitée car les nouveaux normes et standards post-quantiques ont très peu de maturité, et sont susceptibles à évoluer très rapidement. On sera aussi amené à étudier la hybridation efficace - c'est à dire, la fusion des cryptosystèmes pré- et post-quantique - afin de profiter, dans la courte et moyen terme, de la sécurité stable et implantations matures des cryptosystèmes pré-quantiques. Par exemple : la résistance des implantations des nouveux cryposystèmes post-quantiques aux attaques par canaux auxiliaires n'est pas encore au niveau, et dans un premier temps on a besoin de renforcer ces systèmes avec des cryptosystèmes classiques plus résistants.

Principales activités

Recherche en informatique et mathematiques. Production des articles scientifiques et des logiciels Proof-of-Concept (pour utilisation interne au consortium).

Compétences

Ce projet nécessite des compétences de haut niveau en cryptologie et surtout dans la théorie de nombres.

Un très bon niveau d'anglais est essentiel.

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 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

Rémunération

Selon expérience

Informations générales

- **Thème/Domaine :** Algorithmique, calcul formel et cryptologie
  Calcul Scientifique (BAP E)
- **Ville :** Palaiseau
- **Centre Inria :** Centre Inria de Saclay
- **Date de prise de fonction souhaitée :** 2025-09-01
- **Durée de contrat :** 12 mois
- **Date limite pour postuler :** 2025-08-31

Contacts

- **Équipe Inria :** GRACE
- **Recruteur :**
  Smith Benjamin / Benjamin.Smith@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'e?orce 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.