Offer #2025-09151

Chercheur contractuel / Cryptologie

The offer description below is in French

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Tempary Research Position

About the research centre or Inria department

*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.

Context

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.

Assignment

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.

Main activities

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

Skills

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.

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 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

Remuneration

Selon expérience

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology
  Scientific computing (BAP E)
- **Town/city :** Palaiseau
- **Inria Center :** Centre Inria de Saclay
- **Starting date :** 2025-09-01
- **Duration of contract :** 12 months
- **Deadline to apply :** 2025-08-31

Contacts

- **Inria Team :** GRACE
- **Recruiter :**
  Smith Benjamin / Benjamin.Smith@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.