Offer #2025-09202

Doctorant F/H Sécurité de la cryptographie à base de réseaux euclidiens

The offer description below is in French

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

Level of experience : Recently graduated

Context

Dans le cadre d’un partenariat

- projet européen : ERC PARQ

L’ objectif est de

développer et analyser des algorithmes pour résoudre les problèmes liés à la sécurité de la cryptographie à base de réseaux euclidiens, afin d'évaluer la sécurité concrète de ces systèmes.

Les frais de déplacements éventuels seront pris en charge dans la limite du barème en vigueur.

Assignment

Missions :
Avec l'aide de Phong Nguyen, la personne recrutée sera amenée à développer et analyser des algorithmes pour résoudre les problèmes liés à la sécurité de la cryptographie à base de réseaux euclidiens,
afin d'évaluer la sécurité concrète de ces systèmes.
Elle participera également à la rédaction de publications scientifiques et pourra être amené(e) à interagir avec d’autres membres du projet PARQ.

Pour une meilleure connaissance du sujet de recherche proposé :

- Normes de la cryptographie à base de réseaux euclidiens pour la cryptographie post-quantique.

Collaboration :

La personne recrutée sera en lien avec les autres membres du projet PARQ.

Contexte :

Ce sujet de doctorat s'inscrit dans le cadre du projet européen PARQ (ERC Advanced) dirigé par Phong NGUYEN. Le ou la doctorant(e) recruté(e) sera accueilli(e) au DIENS/PSL, au sein de l'équipe de recherche Cascade spécialisée en cryptographie.
Le doctorant bénéficiera d'un encadrement de qualité, d'un accès à des ressources de calcul intensif, et de la possibilité de participer à des conférences et écoles d'été internationales.

Main activities

Principales activités (5 maximum) :

1. Concevoir, implémenter et analyser des algorithmes liés à la cryptographie à base de réseaux euclidiens.
2. Réaliser des expérimentations sur des plateformes de calcul haute performance.
3. Contribuer à la veille scientifique et technologique sur les attaques et contre-mesures en cryptographie post-quantique.
4. Participer aux réunions de l'équipe de recherche et aux collaborations internationales du projet.

Skills

Compétences techniques et niveau requis :

Solide formation en mathématiques et informatique, notamment sur les réseaux euclidiens.
Bonne connaissance des fondements de la cryptographie (classique et post-quantique).
Compétences avancées en développement C++ ; une expérience en programmation GPU (CUDA ou OpenCL) serait un atout.
Rigueur et curiosité scientifique.

Langues : Bon niveau en anglais (lu, écrit, parlé), permettant de lire des articles scientifiques et de communiquer à l'international.

Compétences relationnelles :

Capacité à travailler en équipe et à s’intégrer dans un environnement de recherche dynamique.

Compétences additionnelles appréciées :

Autonomie

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

General Information

- **Theme/Domain :** Algorithmics, Computer Algebra and Cryptology Scientific computing (BAP E)
- **Town/city :** Paris
- **Inria Center :** Centre Inria de Paris
- **Starting date :** 2025-09-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-08-21

Contacts

- **Inria Team :** CASCADE
- **PhD Supervisor :**
  Nguyen Phong-quang / Phong-Quang.Nguyen@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.