



Offre n°2025-09202

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

Type de contrat : Fixed-term contract

Niveau de diplôme exigé : Graduate degree or equivalent

Fonction : PhD Position

Niveau d'expérience souhaité : Recently graduated

Contexte et atouts du poste

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.

Mission confiée

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.

Principales activités

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.

Compétences

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

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

Informations générales

- **Thème/Domaine** : Algorithmics, Computer Algebra and Cryptology
Scientific computing (BAP E)
- **Ville** : Paris
- **Centre Inria** : [Centre Inria de Paris](#)
- **Date de prise de fonction souhaitée** : 2025-09-01
- **Durée de contrat** : 3 years
- **Date limite pour postuler** : 2025-08-21

Contacts

- **Équipe Inria** : [CASCADE](#)
- **Directeur de thèse** :
Nguyen Phong-quang / Phong-Quang.Nguyen@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.