Offre n°2024-08303

Post-Doctoral Research Visit F/M Post-doc on the design and analysis of Symmetric Techniques for Advanced Protocols

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Contexte et atouts du poste

The successfull applicant will work with Léo Perrin within the framework of the ERC grant ReSCALE, that deals with symmetric cryptographic primitives intended to closely integrate with modern public key protocols, called STAPs.

See https://who.paris.inria.fr/Leo.Perrin/rescale/rescale.html for more information about the context.

Mission confiée

With the help of the other members of the ReSCALE team, including Léo Perrin, the recruited person will work on expanding the knowledge of the academic community and of the industry about the best practices when designing "STAP"s.

Principales activités

- Investigate the design and analysis of STAPs.
- Assist in the supervision of the PhD students of the project.

Compétences

Technical skills and level required : good knowledge of Python/SAGE, very good knowledge of symmetric cryptography.

Languages : English

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Informations générales

- **Thème/Domaine :** Algorithmique, calcul formel et cryptologie
  Systèmes d'information (BAP E)
- **Ville :** Paris
- **Centre Inria :** Centre Inria de Paris
- **Date de prise de fonction souhaitée :** 2025-02-01

- **Durée de contrat :** 2 ans
- **Date limite pour postuler :** 2024-11-29

Contacts

- **Équipe Inria :** COSMIQ
- **Recruteur :**
  Perrin Leo / leo.perrin@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.

L'essentiel pour réussir

Advanced knowledge of symmetric cryptography, and ideally some knowledge of the cryptographic protocols requireing STAPS (FHE, MPC...)

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.