Offre n°2025-08946

Post-Doctoral Research Visit F/M Solid Basis for Symmetric Cryptography: Towards a generalization of cryptanalysis techniques, and new links between cryptanalysis and security arguments

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

Type de contrat : CDD

Contrat renouvelable : Oui

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Contexte et atouts du poste

Within the framework of a partnership (you can choose between)

- not applicable,
- collaboration between 2 Inria teams: *****,
- collaboration ({team_Inria} and the start-up *****,
- project/programme/European fund *****,
- public with {French National Research Agency (ANR), local and regional authorities, academic partners, *****]
- value-creation and technology transfer contracts with *****

a package/model/prototype/application/interface/infrastructure/other specify ***
more specifically dedicated to *****.**

Is regular travel foreseen for this post ? "Do not hesitate to make this known and to ensure that "travel expenses are covered within the limits of the scale in force".

Mission confiée

The recruted post-doc will work on the context of the ERC SoBaSyC, both regarding objective 1 (One toolbox to rule them all) and 2 (solid arguments for future desgins).

Symmetric cryptography, essential for enabling secure communications, has benefited from
an explosion of new results in the last two decades, in big part due to several standardization
efforts: many public competitions have been launched since 1997, where the community
proposes cryptographic constructions and simultaneously evaluates their security and per-
formance. The security of symmetric cryptography is based on cryptanalysis: we only gain
confidence in a symmetric cryptographic function through extensive and continuous scrutiny.
However, the current context has not allowed the community to digest all the new findings,
as can be seen from several recurrent issues. The two main ones are:
1) primitives proposed at top-tier venues often get broken by slight modifications of already
known techniques;
2) published cryptanalysis at top conferences sometimes include mistakes or are suboptimal.
They are also often re-invented and re-named.
The main challenge of SoBaSyC is to establish solid bases for symmetric cryptography.
Using cryptanalysis as the starting point, my aim is to unify the knowledge obtained through
the years on the different families of attacks, to transform it with an algorithmic approach
and to endow it with optimizations. The final result will be a toolbox congregating all
our newly proposed optimized algorithms, that will provide the best known attacks on a
given construction, through an easy application. Next, I plan to derive from this algorithmic
approach some theoretical bounds, as well as some properties that I will include in the security
proofs of symmetric constructions, providing more meaningful and realistic security arguments.
This would allow, for the first time, to ensure that any newly proposed primitive or construction
is already resistant to all known attacks, and will considerably increase the confidence on these
functions. It will also save a considerable amount of time and allow the field to

advance, at
last, on solid ground.

Principales activités

Typical post-doc activities, working on reserach topics in the proposed subject, writing papers, participating on a group.

Compétences

Technical skills and level required :

Languages :

Relational skills :

Other valued appreciated :

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 :** 2025-09-01
- **Durée de contrat :** 2 ans
- **Date limite pour postuler :** 2025-06-22

Contacts

- **Équipe Inria :** COSMIQ
- **Recruteur :**
  Naya Plasencia María / Maria.Naya_Plasencia@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.

L'essentiel pour réussir

There you can provide a "broad outline" of the collaborator you are looking for what you consider to be necessary and sufficient, and which may combine :

- tastes and appetencies,
- area of excellence,
- personality or character traits,
- cross-disciplinary knowledge and expertise...

This section enables the more formal list of skills to be completed and 'lightened' (reduced) :

- "Essential qualities in order to fulfil this assignment are feeling at ease in an environment of scientific dynamics and wanting to learn and listen."
- " Passionate about innovation, with expertise in Ruby on Rails development and strong influencing skills. A thesis in the field of **** is a real asset."

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.