Offre n°2025-08955

PhD Position F/M New tools for quantum symmetric cryptanalysis

Type de contrat : Fixed-term contract

Niveau de diplôme exigé : Graduate degree or equivalent

Fonction : PhD Position

A propos du centre ou de la direction fonctionnelle

The Inria Rennes - Bretagne Atlantique Centre is one of Inria's eight centres and has more than thirty research teams. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institute, etc.

Contexte et atouts du poste

The development of quantum computing devices impacts severely the security guarantees of asymmetric cryptography, leading to an ongoing transition to post-quantum, i.e., quantum-secure, cryptosystems. Fortunately, mainstream symmetric primitives are considered robust against hypothetical quantum adversaries. However, our confidence in the security of symmetric cryptosystems is upheld by a rigorous cryptanalysis effort. This effort needs to continue in the context of post-quantum
security.

This PhD position takes place within the QATS project, which studies the cryptanalysis of symmetric primitives (block ciphers, hash functions...) using quantum algorithms. QATS is both focused on the systematization of new attack techniques, and the development of automatic tools that allow to find attacks.

Mission confiée

The PhD candidate will study attacks based on quantum convolution algorithms (which have been used recently in linear cryptanalysis), and their application to block cipher cryptanalysis, as well as the automatization of these techniques.

More information on the research to be carried out in this project as well as relevant bibliographic references are available on this document.

Principales activités

The PhD candidate will contribute to the research activities of the CAPSULE team and the QATS project.

- Design new attack algorithms based on quantum convolutions
- Analyze existing and new attacks and design automatic tools to search for them

The candidate will also communicate her/his work through publications and communications in conferences, workshops or seminars.

Compétences

The ideal candidate will have the following skills:

- A strong level in English for written and oral communication
- Relational skills (working in a team)
- A background in cryptography and / or algorithmics
- Programming skills in Python or other languages
- Notions of quantum computing

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

Rémunération

Salary gross : 2200€

Informations générales

- **Thème/Domaine :** Algorithmics, Computer Algebra and Cryptology
- **Ville :** Rennes
- **Centre Inria :** Centre Inria de l'Université de Rennes
- **Date de prise de fonction souhaitée :** 2025-09-15
- **Durée de contrat :** 3 years
- **Date limite pour postuler :** 2025-07-31

Contacts

- **Équipe Inria :** CAPSULE
- **Directeur de thèse :**
  Schrottenloher Andre / andre.schrottenloher@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.

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

Please submit online : your resume, cover letter and letters of recommendation eventually

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.