2020-02808 - PhD Position F/M Secure Primitives and the Post-Quantum World

Type de contrat : CDD
Niveau de diplôme exigé : Bac + 5 ou équivalent
Fonction : Doctorant

Contexte et atouts du poste
The PhD will take place at Inria-Paris, at the SECRET team (Paris 12ème), in the context of the ERC project QUASYModo², that started in September 2017. A PhD funding is available to this effect.

Mission confiée
As years go by, the existence of quantum computers becomes more tangible and the scientific community is already anticipating the enormous consequences of the induced breakthrough in computational power. Cryptology is one of the affected disciplines. Indeed, the current state-of-the-art asymmetric cryptography would become insecure, and we are actively searching for alternatives. Symmetric cryptography, essential for enabling secure communications, seems much less affected at first sight: its biggest known threat is Grover's algorithm, which allows exhaustive key searches in the square root of the normal complexity. Thus, so far, it is believed that doubling key lengths suffices to maintain an equivalent security in the post-quantum world. The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding cryptanalysis toolbox, which neither exists nor has ever been studied. Next, doubling the key length is not a trivial task and needs to be carefully studied. With the help of this toolbox, the cryptographic community should propose efficient solutions to ensure security in the post-quantum world. This will help prevent the chaos that big quantum computers would generate: being ready in advance will definitely save a great amount of time and money, while protecting our current and future communications.

Principales activités
Therefore, an important challenge to solve is to redesign symmetric cryptography for the post-quantum world. Due to environmental constraints, it is very likely that common users will never take advantage of quantum capabilities, but a powerful adversary will. It is therefore vital that we dispose of primitives that are efficient on classical computers and secure against quantum adversaries. This means that we have definitely a lot of work to do with respect to symmetric cryptography. As symmetric cryptography completely lies in the variety and ever-changing landscape of symmetric cryptanalysis, we are convinced that it is not possible to determine for instance whether doubling the key length might make a concrete cipher secure or not in a post-quantum world, without first understanding how a quantum adversary could attack the primitive. Correctly evaluating the security of symmetric primitives in the post-quantum world cannot be done without a corresponding symmetric cryptanalysis toolbox, which neither exists nor has ever been studied. This PhD will contribute to fill this gap. The aim of this toolbox is two-fold: 1) analyze existing cryptosystems/primitives, and 2) design new ones which will give us confidence in the post-quantum world. The direction of this PhD of adequately preparing symmetric cryptography (and more generally cryptography) for the post-quantum world can logically be decomposed in two main sequential objectives:

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
Informations générales

- **Thème/Domaine** : Algorithmique, calcul formel et cryptologie  
  Systèmes d'information (BAP E)
- **Ville** : Paris
- **Centre Inria** : CRI de Paris
- **Date de prise de fonction souhaitée** : 2020-09-01
- **Durée de contrat** : 3 ans
- **Date limite pour postuler** : 2020-08-01

Contacts

- **Equipe Inria** : COSMIQ
- **Directeur de thèse** :
  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 200 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3500 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 180 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

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."

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.

**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.