Offre n°2024-08327

Post-Doctorant F/H Towards a generalization of cryptanalysis families

Type de contrat : CDD

Contrat renouvelable : Oui

Niveau de diplôme exigé : Thèse ou équivalent

Fonction : Post-Doctorant

Contexte et atouts du poste

Dans le cadre d'un partenariat (vous pouvez choisir entre)

- non pertinent,
- collaboration entre 2 équipes Inria : *****,
- collaboration {Equipe_Inria} et la startup *****,
- projet/programme /fonds européen *****,
- public avec {ANR, collectivités territoriales, partenaires académiques, *****}
- contrats de valorisation et de transfert avec *****

L' objectif est de
produire/ développer/intégrer/ initier/ autre préciser *****
un package / modèle/ prototype/ application/ interface/ infrastructure/ autre préciser *****
plus particulièrement dédié à ******.

Des déplacements réguliers sont prévus pour ce poste ? N'hésitez pas à le signaler et à assurer que "les frais de déplacements seront pris en charge dans la limite du barème en vigueur".

Mission confiée

Cryptanalysis is the foundation of the confidence we have in the cryptographic primitives we use: trying to break them and determining their security margins are fundamental tasks in order to understand the security they can offer.
Symmetric cryptanalysis is a very active and innovative field. There are several families of attacks, the main ones being differential [3] and linear [7], but many others exist and they have all profited from many evolutions through the last years, like MITM (meet-in-the-middle) attacks and their variants (see [6]), differential-linear attacks [1], impossible differential attacks [2, 5] each providing the best results on different constructions.
A new type of attack, differential meet-in-the-middle attacks, was proposed in Crypto 2023 [4], and a recent work under submission proposes some interesting extensions, like using structures to increase the number of attacked rounds.

During the post doc we will study its automamization and generalization of the state test technique.

Principales activités

Cryptanalysis is the foundation of the confidence we have in the cryptographic primitives we use: trying to break them and determining their security margins are fundamental tasks in order to understand the security they can offer.
Symmetric cryptanalysis is a very active and innovative field. There are several families of attacks, the main ones being differential [3] and linear [7], but many others exist and they have all profited from many evolutions through the last years, like MITM (meet-in-the-middle) attacks and their variants (see [6]), differential-linear attacks [1], impossible differential attacks [2, 5] each providing the best results on different constructions.
A new type of attack, differential meet-in-the-middle attacks, was proposed in Crypto 2023 [4], and a recent work under submission proposes some interesting extensions, like using structures to increase the number of attacked rounds.

During the post doc we will study its automamization and generalization of the state test technique.

Compétences

Compétences techniques et niveau requis :

Langues :

Compétences relationnelles :

Compétences additionnelles appréciées :

Avantages

- Restauration subventionnée
- Transports publics remboursés partiellement à 75%
- 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)

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 :** 2025-01-01
- **Durée de contrat :** 12 mois
- **Date limite pour postuler :** 2024-12-04

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'efforce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

L'essentiel pour réussir

Vous pouvez donner là, un portrait à "gros traits" du (de la) collaborateur(trice) attendu(e) : ce que vous voyez comme nécessaire et suffisant et qui peut associer :

- goûts et appétences,
- domaine d'excellence,
- éléments de personnalité ou de caractère,
- savoir et savoir faire transversaux...

Cette rubrique permet de compléter et alléger (réduire) la liste plus formelle des compétences :

- "Se sentir à l'aise dans un environnement de dynamique scientifique, aimer apprendre et écouter sont des qualités essentielles pour réussir cette mission."
- " Passionné(e) par l'innovation, avec une expertise dans le développement Ruby on Rail et une grande capacité de conviction. Une thèse dans le domaine *** constitue un réel atout."

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.