INGÉNIEUR D'ÉTUDES EN MÉTHODES MATHÉMATIQUES POUR L'ÉTUDE DES PRIMITIVES CRYPTOGRAPHIQUES SYMÉTRIQUES AVANCÉES

AFFECTATION

Structure de rattachement : Université Paris 8 - Laboratoire LAGA

Adresse : 2 rue de la Liberté - 93200 Saint-Denis

Catégorie : Equivalent Ingénieur d'étude:/Master
Nature du contrat : Chercheur contractuel

Quotité : 100%.

Durée prévue des missions confiées : durée du contrat : 1 an

DESCRIPTION DU POSTE

DESCRIPTIF DE L'EMPLOYEUR ET DE LA STRUCTURE DE RATTACHEMENT

L'université de Paris 8 est un établissement d'enseignement supérieur qui regroupe 22500 étudiants, 1200 enseignants chercheurs et environ 650 personnels administratifs. L'université exerce des missions de formation et de recherche. Ses activités sont essentiellement tournées vers les sciences humaines et sociales, les arts et le numérique. Concernant la recherche, elle compte 26 unités de recherche et 7 unités mixtes de recherche.

Nous recherchons des candidats ayant une solide formation en mathématiques et intéressés par un poste de recherche financé pendant un an par la partie française du projet CEFIPRA (Centre Indo-Français pour la Promotion de la Recherche Avancée-IFCPAR) au sein de l'équipe AGC3 du laboratoire LAGA. . Il s'adresse notamment aux docteurs ayant terminé leur thèse et qui sont en période creuse en attendant de postuler à des postes d'enseignants (ou des postes permanents similaires).

Les recherches dans ce projet seront menées dans le domaine de la cryptographie. Il se concentrera sur l'étude des primitives cryptographiques symétriques avancées. Il visera à intégrer de nouvelles techniques algébriques pour générer des primitives cryptographiques (optimales ou quasi optimales) dans des cryptosystèmes classiques ou quasi optimaux. post-quantique**.**

MISSIONS DU POSTE

Activités de recherche, tâches à accomplir et résultats attendus

- Nom du projet : «**Méthodes mathématiques pour l'étude des primitives cryptographiques symétriques avancées »**

- Activités de recherche / Contenu du projet de recherche

Le projet est assez ouvert en cryptographie symétrique.Néanmoins, l'accent sera mis sur la mise en œuvre de nouvelles méthodes algébriques et/ou géométriques et le développement d'outils algébriques adaptés à l'étude et à la construction de primitives cryptographiques symétriques et de leurs composantes non linéaires. appelé S-box. L'objectif est d'aider à concevoir de telles primitives, en particulier pour les plates-formes ayant des exigences de mise en œuvre restrictives, telles que des primitives qui restent sécurisées contre les ordinateurs quantiques.

- Tâches à accomplir : Travail de recherche théorique : étude pointue et approfondie de primitives cryptographiques symétriques sélectionnées et développement de méthodes algébriques les générant**.**
- Résultats attendus : Publication d'environ 3 articles de recherche dans des revues de premier plan
- Calendrier prévisionnel Etat de l'art (un mois et demi) puis recherche dans le thème.

1. Etat de l'art (1 mois)

2. étude détaillée et approfondie de primitives cryptographiques symétriques sélectionnées (2 mois)

3. Développement de méthodes algébriques les générant et réaction des résultats (9 mois)

LIENS INTERNES ET EXTERNES

CONDITIONS D'EXERCICE ET, LE CAS ÉCHÉANT, SUJÉTIONS PARTICULIÈRES ATTACHÉES À CE POSTE

Pas de période de mobilité pour assister à des colloques sauf soutenances de thèse ou équivalent.

CONNAISSANCES ET COMPETENCES ATTENDUES

FORMATION ET EXPERIENCE ATTENDUES

Le Diplôme attendu est au minimum un diplôme de Master 2. Un excellent niveau en mathématiques (algèbre, théorie de Galois) et un bon niveau d'anglais sont nécessaires**.**

COMPÉTENCES ATTENDUES

Un excellent niveau en mathématiques (algèbre, théorie de Galois)– une certaine expérience en recherche**.**

PERSONNES À CONTACTER ET ENVOI DES CANDIDATURES

Pour candidater, veuillez adresser un CV et une lettre de motivation à :

job-ref-dgtcua4pts@emploi.beetween.com

- Sihem MESNAGER, porteuse du projet : smesnager@gmail.com
- Sylvie MAZINGHIEN, chargée de recrutement : sylvie.mazinghien@univ-paris8.fr

accompagnés des documents suivants :

-Lettre de motivation

-Curriculum vitae, comprenant éventuellement une liste de publications (max. quatre pages)

-Une déclaration d'intention ou un plan de recherche, max. deux pages (couvrant de préférence un sujet lié aux primitives cryptographiques symétriques)

_Les références

-Certificats/Diplômes : Copie numérisée du certificat de Master original et du relevé de notes et, si nécessaire, traductions officielles en français ou en anglais.

Les candidats éligibles correspondant le mieux au profil attendu pour le poste seront convoqués à un entretien sur place (Université Paris 8) ou à distance. Tous les candidats seront informés rapidement après le processus de sélection.

ANNEXE 2 : Fiche de poste IGE chercheur (en anglais)

POSITION :

ASSIGNMENT

Attached structure: **University of Paris 8 - Laboratory LAGA**

Address: 2 rue de la Liberté - 93200 Saint-Denis

Category: **Research Engineer Equivalent: Master's degree**
Nature of contract: **Contract Researcher**

Quota: 100%.

Expected duration of the assignments : 1 year

JOB DESCRIPTION

DESCRIPTION OF THE EMPLOYER AND OF THE AFFILIATION STRUCTURE

The University of Paris 8 is an institution of higher education with 22,500 students, 1,200 research professors and approximately 650 administrative staff. The university carries out training and research missions. Its activities are mainly focused on human and social sciences, arts and digital technology. As far as research is concerned, it has 26 research units and 7 mixed research units.

We seek candidates with a solid background in mathematics interested in a research position funded for one year by the French part of the CEFIPRA project (Indo-French Center for the Promotion of Advanced Research-IFCPAR) within the AGC3 team from the LAGA laboratory. It is aimed, in particular, at doctors who have completed their thesis and are in a slack period while waiting to apply for teaching positions (or similar permanent positions).

Research in this project will be conducted in the field of cryptography. It will focus on the study of advanced symmetric cryptographic primitives. It will aim to integrate new algebraic techniques to generate cryptographic primitives (optimal or quasi-optimal) in classical or quasi-optimal cryptosystems post-quantum.

TASKS OF THE POST

Research activities, tasks and expected results

- Name of the project: "Mathematical Methods for the Study of advanced symmetric cryptographic primitives. »

- Research activities / Content of the research project

The project is entirely open in symmetric cryptography. Nevertheless, the emphasis will be placed on making up new algebraic and/or geometric methods and developing algebraic tools adapted to the study and construction of symmetric cryptographic primitives and their non-linear components, called S-box. The goal is to help design such primitives, particularly for platforms with restrictive implementation requirements, such as primitives that remain secure against quantum computers.

- Tasks to be performed: Theoretical research work: a cutting-edge and in-depth study of selected symmetric cryptographic primitives and the development of algebraic methods generating them.
- Expected results: publication of approximately 3 research articles in leading journals

- Provisional timetable
- 1. State of the art (1 month)
- 2. detailed and in-depth study of selected symmetric cryptographic primitives (2 months)
- 3. Development of algebraic methods generating them and reaction to the results (9 months)

INTERNAL AND EXTERNAL LINKS

For more scientific details, you can contact the person responsible for the French side, Prof. Sihem Mesnager: smesnager@univ-paris8.fr

CONDITIONS OF SERVICE AND, WHERE APPROPRIATE, PARTICULAR HARDSHIP ATTACHED TO THE POST

There is no mobility period to attend conferences except thesis defences or equivalent.

EXPECTED KNOWLEDGE AND SKILLS

EXPECTED TRAINING AND EXPERIENCE

The expected Diploma is at least a Master 2 —some experience in research.

EXPECTED SKILLS

An excellent level of mathematics (algebra, Galois theory) and good English are necessary. – some research experience.

CONTACT PERSON AND APPLICATION FORM

To apply, please send a CV and a letter of motivation to

job-ref-dgtcua4pts@emploi.beetween.com

Interested candidates must send their application by email to smesnager@univ-paris8.fr and Sylvie MAZINGHIEN, recruitment officer : sylvie.mazinghien@univ-paris8.fr **accompanied by the following documents:**

-Cover letter

-Curriculum vitae, possibly including a list of publications (max. four pages)

-A statement of intent or research plan, max. two pages (preferably covering a topic related to symmetric cryptographic primitives)

-Reference letters

-Certificates/Diplomas: Scanned copy of the original Master's certificate and transcript and, if necessary, official translations into French or English.

Eligible candidates who match the expected profile will be invited to an on-site interview (University Paris 8) or remotely. All applicants will be informed promptly after the selection process.