Entité(s)/DER : DER Informatique et Laboratoire Méthodes Formelles

Intitulé du profil : Méthodes formelles et sécurité

Discipline : Informatique

Statut : ☒ MCF ☐ PR

Introduction

L'Ecole normale supérieure Paris-Saclay (ENS Paris-Saclay) est attachée à recruter des enseignants-chercheurs et des enseignants sans obligation de recherche inscrivant pleinement leurs projets dans les missions de l'établissement, qui sont la formation des normaliens aux métiers de l'enseignement supérieur et de la recherche et le développement d'une recherche scientifique au plus haut niveau. Un des objectifs de l'Ecole est de conduire 80% de ses normaliens au doctorat.

Les enseignant.es de l'ENS Paris-Saclay recruté.es doivent se positionner au meilleur niveau de leur discipline et avoir des expériences d'enseignement et de recherche significatives. Une connaissance large de leur champ disciplinaire est attendue pour assurer aux normaliens l'acquisition d'une véritable culture scientifique dans toutes les phases de la formation.

La personne recrutée devra s'inscrire dans les projets stratégiques de l'École.

L'École propose des conditions de travail favorables à ses personnels enseignants et recherche : réputation d'excellence de sa recherche et de ses élèves, qualité des infrastructures, niveau de la dotation per capita des laboratoires, implication dans les opérations du Programme d'investissements d'avenir, conditions de participation dans les responsabilités d'intérêt collectif.

ENS Paris-Saclay www.ens-paris-saclay.fr 4 avenue des sciences CS30008 91192 Gif-sur-Yvette Cedex

Description des entités/du département de rattachement

Les membres du département d'enseignement et de recherche (DER) en informatique effectuent leur activité de recherche dans le Laboratoire Méthodes Formelles (LMF – https://lmf.cnrs.fr), laboratoire né le 1er janvier 2021 de la volonté de ses tutelles — Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria et CentraleSupélec — de créer un pôle ciblé sur les méthodes formelles.

Le LMF est formé de l'ancien Laboratoire Spécification et Vérification (LSV, ENS Paris-Saclay, CNRS, Inria) et de l'équipe Vals de l'ancien Laboratoire de Recherche en Informatique (LRI, Université Paris-Saclay, CNRS, Inria, CentraleSupélec).

Les méthodes formelles permettent de raisonner rigoureusement sur les systèmes informatiques (programmes, langages, protocoles, algorithmes, ...), afin d'apporter des garanties sur leurs fonctionnements et ainsi assurer la haute qualité des systèmes ou logiciels développés (correction, sûreté, sécurité, réutilisabilité, etc.). Le LMF s'appuie sur des paradigmes de calcul des plus classiques aux plus novateurs comme l'informatique quantique.

Le DER propose une formation orientée vers les fondements de l'informatique préparant en particulier aux métiers de la recherche scientifique (https://lmf.cnrs.fr/deptinfo-ens).
Cette formation comporte une année de licence (L3) et deux années de master recherche, en général dans le cadre du master parisien de recherche en informatique (MPRI) et une année de formation complémentaire (préparation à l'agrégation, formation dans une autre discipline ou année de recherche pré-doctorale à l'étranger).
Elle permet aussi de suivre un cursus mixte mathématiques/informatique à la carte, avec la possibilité de passer l'agrégation de mathématiques ou la nouvelle agrégation d'informatique.
À l'issue de cette solide formation, les étudiants et élèves normaliens ont la capacité de suivre des carrières diversifiées : maîtres de conférences ou chargés de recherche, participation à un département recherche et développement d'une entreprise, enseignement en lycée, classes préparatoires ou dans le supérieur via l'agrégation.

Profil enseignement

Le ou la candidat.e devra témoigner de compétences en informatique théorique avec une motivation pour les applications.

Elle/Il devra s'investir dès la rentrée dans les enseignements qui constituent le socle de connaissances de nos élèves : algorithmique, calculabilité et complexité, logique et programmation.

Elle/Il devra participer à l'enseignement des modules d'option en M1 (complexité avancée, réécriture, langages formels, génie logiciel), proposer des sujets et accompagner la réalisation des projets en L3 et M1 (logique, compilation, programmation, génie logiciel), participer avec l'équipe pédagogique à la mise en place des enseignements de la future préparation à l'agrégation d'informatique.

Le ou la candidat.e pourra être amené.e à effectuer des interventions et/ou des enseignements disciplinaires en langue anglaise.

ENS Paris-Saclay www.ens-paris-saclay.fr 4 avenue des sciences CS30008 91192 Gif-sur-Yvette Cedex

Profil recherche

Le ou la candidate.e devra scientifiquement s'intégrer dans une ou plusieurs des thématiques du laboratoire (https://lmf.cnrs.fr/Research/).
Sans que cela soit exclusif, une priorité sera donnée pour la thématique « Méthodes formelles et sécurité ».

La sécurité et la protection de la vie privée constituent des enjeux sociétaux importants, avec des besoins grandissants aussi bien en termes de sécurisation des objets communicants ou des protocoles comme les protocoles RFID, qu'en terme de protection des données personnelles ou confidentielles.

Le LMF souhaite renforcer sa thématique « Méthodes formelles et sécurité », qui s'intéresse actuellement à la modélisation et à l'analyse des primitives cryptographiques et des protocoles qui les utilisent, ainsi qu'à l'analyse de leurs implémentations. L'approche que nous suivons s'appuie sur :

— la conception des briques de base que sont les primitives cryptographiques dédiées à l'authentification (signatures aveugles, signatures de groupe ou identifiants anonymes) ou à la confidentialité (chiffrement homomorphe, chiffrement fonctionnel ou mix-nets) ;
— l'assemblage de ces primitives en protocoles conçus pour assurer la sécurité mais aussi la confidentialité des télécommunications ou des applications émergentes, telles que le vote électronique, le service cloud ou les données massives (big data).

L'objectif est d'analyser la sécurité de ces protocoles de manière la plus automatisée possible. Cette analyse peut permettre de prouver la sécurité ou bien de mettre en évidence des attaques. Son caractère automatisé est essentiel pour mettre en évidence des attaques complexes qu'une analyse manuelle ne permettrait pas toujours d'identifier, et pour dérouler des preuves elles aussi complexes.
Cette approche s'intègre dans l'expertise plus globale du LMF, en modélisation et en preuve automatisée. Des projets d'ouverture liant les méthodes formelles et la sécurité, hors protocoles cryptographiques, seront également les bienvenus.

ENS Paris-Saclay www.ens-paris-saclay.fr 4 avenue des sciences CS30008 91192 Gif-sur-Yvette Cedex

Mise en situation professionnelle

Forme	X Présentation à vocation pédagogique ❑ Séminaire de présentation des travaux de recherche
Durée de préparation	Sans objet
Durée de la mise en situation	**10 minutes**
Publicité	En présence des membres du CDS uniquement
Choix des thèmes exposés	Imposés et communiqués au candidat lors de sa convocation à l'audition

Contacts

SIGHIREANU Mihaela
Directrice du DER Informatique
mihaela.sighireanu@ens-paris-saclay.fr

BOUYER Patricia
Directrice du LMF
patricia.bouyer@ens-paris-saclay.fr