UNIVERSITE VERSAILLES/SAINT-QUENTIN	Référence GALAXIE : 4308

Numéro dans le SI local :	
Référence GESUP :	
Corps à l'issue de la titularisation :	Professeur des universités
Article :	CPJ
Chaire :	Non
Section 1 :	27-Informatique
Section 2 :	
Section 3 :	
Intitulé du contrat et du poste à pourvoir :	Le projet scientifique CRYPTALGAPP (Cryptologie : de l•algebre aux applications) vise a renforcer le potentiel de l'equipe LMV/CRYPTO en cryptologie fondamentale et/ou en cryptologie appliquee. Le projet scientifique precis est ouvert au sein de l•equipe, et devra mettre en evidence des liens avec les axes de recherche de l•equipe..
Nature et objet de l'appel à projet de recherche et d'enseignement :	La personne recrutée aura une charge d¿enseignement de 96h eq. TD par an. Elle prendra progressivement en charge le développement et la coordination d¿unités d'enseignement portées par l'UVSQ concernant la cryptographie et/ou la cybersécurité au sein des masters de l'université Paris-Saclay.
Nature et objet de l'appel à projet de recherche et d'enseignement (version anglaise) :	The candidate will integrate the CRYPTO research team, within the Computer Science Department and the LMV laboratory (UMR CNRS 8100), whose main interests are cryptography and information security.
Research fields EURAXESS :	Computer science Informatics
Montant du financement associé :	
Durée prévisible du projet :	
Implantation du poste :	0781944P - UNIVERSITE VERSAILLES/SAINT-QUENTIN
Localisation :	VERSAILLES
Code postal de la localisation :	
Etat du poste :	Vacant
Adresse d'envoi du dossier :	DRH - SERVICE ENSEIGNANTS 78035 - VERSAILLES CEDEX
Contact administratif : **N° de téléphone :** **N° de Fax :** **Email :**	SERVICE ENSEIGNANTS 01.39.25.78.35 01.39.25.78.65 01.39.25.41.78 drh.enseignant@uvsq.fr
Date d'ouverture des candidatures :	05/05/2023
Date de fermeture des candidatures :	05/06/2023, 16 heures 00, heure de Paris
Date de prise de fonction :	01/09/2023
Mots-clés :	
Profil enseignement : **Composante ou UFR :** **Référence UFR :**	UFR DES SCIENCES
Profil recherche : **Laboratoire 1 :**	UMR8100 (200111674P) - Laboratoire de mathématiques de Versailles
Application Galaxie	OUI
Informations complémentaires :	Seuls seront convoqués à l'audition, les candidats préalablement sélectionnés sur dossier par la commission

Poste ouvert également aux personnes 'Bénéficiaires de l'Obligation d'Emploi' mentionnées à l'article 27 de la loi n° 84-16 du 11 janvier 1984 modifiée portant dispositions statutaires relatives à la fonction publique de l'Etat (situations de handicap).

Le poste sur lequel vous candidatez est susceptible d'être situé dans une "zone à régime restrictif" au sens de l'article R.413-5-1 du code pénal. Si tel est le cas, votre nomination et/ou votre affectation ne pourront intervenir qu'après

autorisation d'accès délivrée par le chef d'établissement, conformément aux dispositions de l'article 20-4 du décret n°84-431 du 6 juin 1984.

Le profil détaillé se trouve en pages suivantes

Fiche de poste Chaire de professeur junior

Décret n° 2021-1710 du 17 décembre 2021 relatif au contrat de chaire de professeur junior prévu par l'article L. 952-6-2 du code de l'éducation et par l'article L. 422-3 du code de la recherche.

Corps dans lequel l'intéressé a vocation à être titularisé : **Professeur des Universités**
Profil de publication *(intitulé du contrat et du poste concerné)* : **CHAIRE DE PROFESSEUR JUNIOR en Cryptologie**
Section(s) CNU correspondante(s) : 27
Localisation : UFR des Sciences / Laboratoire LMV (UMR CNRS 8100) / Equipe CRYPTO

Nature et objet du projet de recherche : Le projet scientifique CRYPTALGAPP (Cryptologie : de l'algèbre aux applications) vise à renforcer le potentiel de l'équipe LMV/CRYPTO en cryptologie fondamentale et/ou en cryptologie appliquée. Le projet scientifique précis est ouvert au sein de l'équipe, et devra mettre en évidence des liens avec les axes de recherche de l'équipe

Nature et objet du projet d'enseignement proposé : La personne recrutée aura une charge d'enseignement de 96h eq. TD par an. Elle prendra progressivement en charge le développement et la coordination d'unités d'enseignement portées par l'UVSQ concernant la cryptographie et/ou la cybersécurité au sein des masters de l'université Paris-Saclay. Elle pourra également contribuer aux enseignements d'informatique en licence et à leur organisation au besoin.

Partenaires :

Montant du financement associé : 475 K€ (incluant le salaire du recruté sur la période contractuelle et un apport de l'ANR)

Durée prévisible du projet : 3 à 5 ans

- **Job profile et EURAXESS :**

Job profile (résumé en deux lignes maxi du profil en anglais) : The candidate will integrate the CRYPTO research team, within the Computer Science Department and the LMV laboratory (UMR CNRS 8100), whose main interests are cryptography and information security.

Research fields Euraxess (cf tableau de codification dans les documents annexes) : Computer science - Other

- **Profil du poste:**

Profil enseignement : Les enseignants-chercheurs de l'équipe CRYPTO du LMV sont déjà très investis dans les enseignements des graduate schools Maths, et Informatique et Sciences du numérique de l'université Paris-Saclay. Ils coordonnent le master SeCReTS (Sécurité des Contenus, des Réseaux, des Télécommunications et des Systèmes), avec un réseau de plus de 530 alumni occupant des postes clés dans des entreprises ou organismes de haute technologie spécialisés en cybersécurité, et co-animent le master Algèbre Appliquée, dont sont issus une quarantaine de docteurs en cryptographie. Cela illustre tout le potentiel de développement de ces formations, et a déjà valu à l'équipe d'être sélectionnée dans le volet Cybersécurité de l'appel « Compétences et métiers d'avenir ». La personne recrutée aura une charge d'enseignement de 96h eq. TD par an. Elle prendra progressivement en charge le développement et la coordination d'unités d'enseignement portées par l'UVSQ concernant la cryptographie et/ou la cybersécurité au sein des masters de l'université Paris-Saclay. Elle contribuera également aux enseignements d'informatique en licence et à leur organisation au besoin. Le projet d'enseignement proposé devra refléter l'ambition du projet scientifique.

Mots-clés enseignement : Cryptographie, sécurité informatique, cybersécurité, informatique

Composante/UFR : UFR des Sciences
Département d'enseignement : Informatique
Lieu(x) d'exercice : Versailles

Contact Equipe pédagogique : Louis Goubin louis.goubin@uvsq.fr

Projet et Profil recherche : La cryptographie est une composante majeure de la cybersécurité garantissant un monde numérique sûr, et un moyen de protection des droits des citoyens. Elle repose dans un premier temps sur un ensemble d'algorithmes (avant un deuxième temps qui est la mise en œuvre opérationnelle de ces algorithmes sous forme de protocole puis d'un troisième temps d'implémentation effective) dont l'efficacité dépend de la preuve d'impossibilité de résoudre « en temps acceptable » certains problèmes mathématiques. Le projet scientifique vise à renforcer le potentiel de l'équipe LMV/CRYPTO en cryptologie fondamentale et/ou en cryptologie appliquée. Le projet scientifique précis est ouvert au sein de l'équipe, et devra mettre en évidence des liens avec les axes de recherche de l'équipe. À titre d'exemple, la cryptographie post-quantique peut concerner les axes 1 (complexité de problèmes algébriques dans le contexte de l'algorithmique quantique), 2 (nouvelles techniques de cryptanalyse quantique dans le cas symétrique), 3 (étude de cryptosystèmes conçus pour résister aux ordinateurs quantiques) et 4 (attaques par canaux auxiliaires). Il est attendu que chaque candidat(e) propose un projet de recherche ambitieux, tourné vers l'international, et précisant une stratégie d'implémentation.

Mots-clés recherche : Cryptologie, cryptographie, cryptanalyse

Contact pour le projet de recherche : Louis Goubin louis.goubin@uvsq.fr

Description et stratégie laboratoire :

Au sein du laboratoire LMV (UMR 8100 CNRS-UVSQ), les activités de recherche de l'équipe CRYPTO (Cryptologie et sécurité de l'information) s'organisent selon 4 axes : Algorithmique fondamentale pour la cryptographie, Constructions prouvées en cryptographie symétrique, Algorithmes et protocoles cryptographiques pour les applications émergentes, et Méthodes cryptographiques pour la sécurité des codes embarqués.
Dans ce contexte où se multiplient de nombreux défis scientifiques transverses entre ces quatre axes, cette chaire de professeur junior a pour objectif de : 1) Renforcer la compétence théorique forte et reconnue de l'équipe en cryptologie fondamentale (symétrique et asymétrique), s'appuyant sur une connaissance cryptanalytique fine des primitives mathématiques mises en jeu, tout en tenant compte de modèles de sécurité de plus en plus exigeants (cryptographie post-quantique, cryptographie en boîte blanche et obfuscation de code) et de fonctionnalités de plus en plus complexes. 2) Développer leur déclinaison sur des applications où la cryptologie est cruciale pour garantir la sécurité des données personnelles et créer la confiance numérique : le *cloud computing*, les systèmes embarqués et l'internet des objets ou encore les technologies de type *blockchain*.

Informations complémentaires :

- **Modalités de candidature**

Les conditions requises de la part des candidats :

- Être titulaire d'un doctorat ou à défaut titulaire d'une équivalence avec le doctorat de leurs diplômes universitaires, qualifications et titres, attribuée par décision du conseil académique réuni en formation restreinte.

En outre, il est recommandé :

- D'avoir accompli au moins 3 ans d'activité scientifique après la thèse,
- Pour les titulaires d'un doctorat en France, d'avoir une expérience de mobilité à l'étranger significative.

Conformément à l'article 18-3 de l'arrêté du 22 février 2022, le dossier de candidature comporte les documents suivants :

1) Une pièce d'identité avec photographie recto verso ;

2) Une pièce attestant de la possession d'un doctorat, tel que prévu à l'article L612-7 du code de l'éducation, ou pour les candidats qui ne sont pas titulaires d'un doctorat, d'un diplôme dont l'équivalence est reconnue par le Conseil académique réuni en formation restreinte de l'UVSQ, selon la procédure fixée au 1°) de l'article 5 du décret 2021-1710 du 17 décembre 2021 ;

3) Le rapport de soutenance du diplôme produit signé des rapporteurs si possible (Rapport de soutenance de la thèse) ;

4) La fiche de candidature CPJ accessible sur le portail GALAXIE, à déposer dans la partie «Titres et travaux». *Attention, il est rappelé l'importance du développement de la partie relative au projet de recherche et pédagogique.*

5) Pièces facultatives : présentation analytique, travaux, ouvrages, articles…

Les documents administratifs ainsi que le rapport de soutenance rédigés en tout ou partie en langue étrangère sont accompagnés d'une traduction en langue française dont le candidat atteste la conformité sur l'honneur. À défaut, le dossier est déclaré irrecevable.
La traduction de la présentation analytique ainsi que des travaux, ouvrages, articles et réalisations est facultative.

Les dossiers de candidature devront être déposés sur Galaxie (module FIDIS (fil de l'eau)*1) selon le calendrier disponible sur le site de l'Université de Versailles Saint-Quentin-en-Yvelines ainsi que sur le portail Galaxie, soit du 05/05/2023 au 05/06/2023 à 16h.

Les candidat(e)s établissent un dossier en version numérique, destiné à Monsieur le Président de l'Université de Versailles Saint-Quentin-en-Yvelines et accessible aux membres de la commission de sélection.
Aucun dossier papier ne sera accepté.

Seuls seront convoqués à l'audition les candidats préalablement sélectionnés sur dossier par la commission de sélection.

- **Modalités d'organisation des auditions**

Sélection des candidats autorisés à passer l'audition par le jury de recrutement

Mise en situation professionnelle :

☐ oui ☑ **non**

Pour les candidats autorisés à passer l'audition :

- Audition devant le jury de recrutement : 30' de présentation (bilan/projet, Recherche/Enseignement, intégration au LMV/équipe CRYPTO) + 20' de questions. Pour cette étape, le présentiel est nettement préféré. Le jury appréciera en particulier le projet d'enseignement, le projet de recherche, et le projet d'intégration au sein de l'équipe CRYPTO du LMV.

[1] **Lors de la recherche de postes, les chaires de professeurs juniors se distingueront des autres par l'article de recrutement (CPJ).*

- les modalités pratiques seront données lors de la convocation.

Période contractuelle de 3 à 5 ans selon l'expérience du candidat (voir Annexe 1)

Une expérience postdoctorale de 3 ans après la thèse est recommandée, de même qu'une expérience à l'étranger.

Les modalités de titularisation dans le corps des professeurs d'université respecteront le décret mentionné en tête de ce document et sont données à titre indicatif pour information des candidats dans la suite de ce document en Annexe 2 (seule la convention signée fera foi).

Annexe 1 : Conditions indicatives d'exercices spécifiques du titulaire de la CPJ au LMV

- Intégration dans l'équipe CRYPTO du LMV
- 96h eqTD d'enseignement / an en moyenne (par exemple, pour N années de CDD : 64h l'année 1, 128h l'année N et 96h les autres années)
- Participation à la vie scientifique de l'équipe CRYPTO du LMV
- Participation à la vie des équipes pédagogiques de l'université (UFR des Sciences)
- Prise de responsabilités collectives coté recherche ou formation
- Bilan annuel d'activité avec le référent laboratoire.
- Rédaction d'un rapport final bilan-perspective en fin de période contractuelle et soutenance de ce rapport devant le jury pour la titularisation.
- Suivi du processus par un référent permanent de la direction du LMV.

Annexe 2 : Critères de titularisation du titulaire de la CPJ au LMV

1. Critères qualitatifs

- Mise en place d'une recherche productive, originale, avec une autonomie individuelle
- Capacité de créer/entretenir des collaborations de recherche du local jusqu'à l'international
- Intégration dans l'équipe CRYPTO en recherche et en enseignement

2. Critères quantitatifs

- Publications
  Au moins 1 publication par an en moyenne dans une conférence internationale avec comité de lecture ou un journal international avec comité de lecture

- Projets de recherche
  Pendant la période contractuelle, être porteur d'un projet d'envergure nationale (ANR, …) ou WP leader (minimum) d'un projet européen (e.g. Horizon Europe). Dans le cas contraire, démontrer sa capacité à construire un projet scientifique de qualité au niveau national ou international via la réponse comme porteur de projet à des Appels à projet ANR, Horizon Europe, …

- Encadrement doctoral
  Encadrement d'au moins un étudiant chaque année (thèse, stage de master) avec au moins une thèse co-encadrée pendant la période contractuelle

- Reconnaissance internationale
  Au moins un item parmi les suivants : talk invité dans une conférence, reviewer d'articles pour une conférence ou une revue internationale à comité de lecture, un prix ou une distinction, un article particulièrement cité (>50)

- Responsabilité en enseignement
  Au moins 1 unité d'enseignement en responsabilité pour chaque année universitaire de la période contractuelle ou la responsabilité d'un parcours / filière

- Actions de diffusion vers le grand public et/ou la société.
  Au moins une action de vulgarisation ou de diffusion grand public sur la période contractuelle

- Rendu (à la fin de la période contractuelle)
  Rapport final comprenant la synthèse des travaux (recherche et formation) menés pendant la période contractuelle (env.

10 pages) et prospectives à 5 ans (env. 10 pages). Ce rapport est à considérer dans l'esprit de l'habilitation à diriger des recherches.

3. Critères quantitatifs

- À l'issue de la période contractuelle, le jury de titularisation examine le rapport final et auditionne le candidat à la titularisation. Le jury apprécie les différents critères qualitatifs et quantitatifs, et décide de la titularisation ou non.

- Remarque : les critères chiffrés sont répartis librement sur l'ensemble de la période contractuelle.