

Numéro dans le SI local :	
Référence GESUP :	
Corps :	Maître de conférences
Article :	26-I-1
Chaire :	Non
Section 1 :	27-Informatique
Section 2 :	
Section 3 :	
Profil :	Cryptologie et sécurité de l'information
Job profile :	The candidate will be teaching in the computer science department of the • UFR Sciences •, in particular in • Licence • and Master of Computer Science. The candidate will conduct research in one of the following fields: design, analysis and security proofs for cryptographic algorithms and...
Research fields EURAXESS :	Computer science Other
Implantation du poste :	0781944P - UNIVERSITE VERSAILLES/SAINT-QUENTIN
Localisation :	VERSAILLES
Code postal de la localisation :	
Etat du poste :	Vacant
Adresse d'envoi du dossier :	UVSQ DRH - SERVICE ENSEIGNANTS 55 AVENUE DE PARIS 78035 - VERSAILLES CEDEX
Contact administratif :	SERVICE ENSEIGNANTS
N° de téléphone :	01.39.25.79.59 01.39.25.78.35
N° de Fax :	01.39.25.41.78
Email :	drh.enseignant@uvsq.fr
Date de prise de fonction :	01/09/2019
Mots-clés :	
Profil enseignement :	
Composante ou UFR :	UFR des Sciences
Référence UFR :	
Profil recherche :	
Laboratoire 1 :	UMR8100 (200111674P) - Laboratoire de mathématiques de Versailles
Dossier Papier	NON
Dossier numérique physique (CD, DVD, clé USB)	NON
Dossier transmis par courrier électronique	NON e-mail gestionnaire
Application spécifique	OUI URL application https://dematec.dsi.uvsq.fr/DematEC

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

PROFIL DE POSTE

Recrutement enseignants-chercheurs

Composante : UFR Sciences Département : Informatique Laboratoire : LMV	Localisation : Versailles
---	----------------------------------

Identification du poste	Etat du poste
Nature : MCF N° emploi Galaxie : 4184 Section CNU : 27	<input checked="" type="checkbox"/> Vacant <input type="checkbox"/> Susceptible d'être vacant Date d'affectation : 01/09/2019

Concours : <input checked="" type="checkbox"/> MCF ou <input type="checkbox"/> PR

Profil pour publication : Cryptologie et sécurité de l'information

Enseignement
Le (la) candidat.e recruté.e fera son enseignement au sein des filières gérées par le département Informatique de l'université. Il aura vocation à enseigner diverses facettes de l'informatique (programmation, cryptographie, ...etc) principalement en Licence d'informatique, Master 1 informatique et Master 2 informatique. Il/elle interviendra notamment dans le parcours SeCReTS de la mention de master Informatique de l'UPSaclay.

Recherche

- Le ou la candidat.e devra s'intégrer dans l'équipe "Cryptologie et Sécurité de l'Information" du laboratoire LMV de l'UVSQ (UMR CNRS 8100).
- L'activité de recherche pourra s'inscrire dans un ou plusieurs des axes suivants :
 - Schémas asymétriques (courbes elliptiques, couplages, polynômes multivariés, réseaux euclidiens, chiffrement homomorphe, cryptographie post-quantique, ...)
 - Preuves de sécurité pour les protocoles à clé secrète ou à clé publique ;
 - Conception et cryptanalyse de fonctions de hachage et d'algorithmes de chiffrement symétrique ;
 - Attaques par canaux auxiliaires : modélisation et contre-mesures ;
 - Cryptographie et calcul intensif, cryptanalyse, bases de Gröbner, réduction de réseaux ;
 - Algorithmes et protocoles pour les RFID, les cartes à microprocesseur et les systèmes embarqués ;
 - Sécurité des logiciels, rétro-conception et obfuscation de code.

Autre

- Le ou la candidat.e devra s'impliquer dans l'organisation et le suivi de projets de recherche collaboratifs (ANR, FUI, projets européens, ...).
- Il/elle lui sera demandé d'assurer à terme raisonnable des responsabilités pédagogiques ou administratives.

Contacts pour le profil :
Enseignement : Sandrine Vial (sandrine.vial@uvsq.fr)
Recherche : Louis Goubin (Louis.Goubin@uvsq.fr)

Traduction en anglais (4 lignes maximum) : Job Profile
Teaching: The candidate will be teaching in the computer science department of the « UFR Sciences », in particular in « Licence » and Master of Computer Science.
Research: The candidate will conduct research in one of the following fields: design, analysis and security proofs for cryptographic algorithms and protocols, physical attacks, lightweight crypto, software security.

Research Fields (cf annexe 3 ci-jointe) :
Computer Science: Other (Cryptology / Information Security)