PROFIL DE POSTE
Recrutement enseignants-chercheurs
(Annexe 2)

Composante : UFR des Sciences ***Département : Informatique*** ***Laboratoire : LMV*** ***Labo ZRR :*** ☑ OUI ☐ NON	***Localisation : Versailles***

Identification du poste	***Etat du poste***
Nature : PR N° emploi : 4338 Section CNU : 27	☑ Vacant ☐Susceptible d'être vacant Date d'affectation : 01/09/2024

Concours : ☐ **MCF** **ou** ☑ **PR** **ou** ☐ **PR au titre du 46-3 °**

Profil pour publication : Cryptologie et sécurité de l'information

Enseignement

L'enseignement devra être fait au sein des filières d'enseignement du Département Informatique de l'UFR des Sciences au niveau Licence et Master, en particulier les cours relevant de la Cryptographie en Licence Informatique et dans le Master SeCReTS.

Recherche

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.

- 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 ;
  - Cryptographie et calcul intensif, cryptanalyse, bases de Gröbner, réduction de réseaux ;
  - Conception et cryptanalyse de fonctions de hachage et d'algorithmes de chiffrement symétrique ;
  - Cryptanalyse et algorithmique quantique ;
  - Attaques par canaux auxiliaires : modélisation et contre-mesures ;
  - Cryptographie en boîte blanche 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, projets européens, ...) et dans la valorisation de la recherche.
- Il lui sera demandé d'assurer à terme raisonnable des responsabilités pédagogiques ou administratives.

Contacts pour le profil :
Enseignement : Franck Quessette (franck.quessette@uvsq.fr)
Recherche : Louis Goubin (louis.goubin@uvsq.fr)

Traduction en anglais (4 lignes maximum) : Job Profile

Teaching: The candidate will teach in the Computer Science Department: Licence and/or Master.
Research: The candidate will conduct research in one of the following fields: asymmetric schemes, post-quantum cryptography, security proofs, design and cryptanalysis of symmetric schemes, cryptanalysis and quantum computing, side channel attacks, white-box cryptography and code obfuscation.

Research Fields (cf annexe 3 ci-jointe) :

Computer Science: Other (Cryptology / Information Security)