RECRUTEMENT ENSEIGNANTS- CHERCHEURS – CAMPAGNE 2022
PROFIL DE POSTE

Identification du poste

Corps : ☐ Professeur des Universités ■ Maître de conférences

Profil publié : Cybersécurité et sécurité du calcul

Job profile (150 caractères maximum) : Cybersecurity and computational security

Section(s) CNU publiées : 26/27

Date de prise de fonction : 1/9/2022

Localisation du poste : UFR IM2AG, Laboratoire Jean Kuntzmann (LJK)

Euraxess research field :

Chaire : ☐ oui ■ non Organisme paritaire (si Chaire):

Mots-clés (EURAXESS) :
1- Sécurité
2- Mathématiques
3- Informatique
4- Cryptanalyse Algébrique

Sections CNU associées **définissant la discipline** (information interne utile qui n'apparait pas lors de la publication) : 26 et 27

Enseignement

Composante/UFR : : IM2AG
URL composante : https://im2ag.univ-grenoble-alpes.fr
Contact
Prénom/Nom : Eric Blayo, Lydie du Bousquet
Mail : Eric.Blayo@univ-grenoble-alpes.fr; lydie.du-bousquet@univ-grenoble-alpes.fr
Tél: 04 57 42 17 11 ; 04 57 42 14 86

Descriptif enseignement :

Les formations de l'UFR IM2AG couvrent une très grande partie des domaines des mathématiques fondamentales jusqu'à l'informatique ainsi que des domaines à la croisée des disciplines. Les formations de l'UFR sont sous la responsabilité d'écoles de formation : école de mathématiques, école d'informatique et école de mathématiques appliquées qui sera l'école de référence du (de la) maître de conférences recruté(e).

Le/la personne recruté.e s'investira dans un large éventail d'enseignements, en informatique et en mathématique-informatique, en parcours Licence et Master à l'UFR IM2AG. Plus particulièrement dans la Licence 3 Maths-Info, les Masters 1 informatique et mathématiques appliquées ainsi que le Master 2 CyberSécurité conjoint avec l'ENSIMAG.

Teaching profile: (version anglaise obligatoire)

The teaching courses at the UFR IM2AG cover a wide domain from fundamental mathematics to computer science as well as fields at the crossroads of disciplines. Teaching at UFR is under the responsibility of so called "schools": school of mathematics, school of computer science and school of applied mathematics, the last being the school of reference for the recruited lecturer.

The person recruited will be involved in a wide range of teaching in computer science and mathematics, in the Bachelor's and Master's courses at the UFR IM2AG. More particularly in the Licence 3 "Maths-Info", the Masters 1 "computer science" and "applied mathematics" as well as the Master 2 "CyberSecurity" (joint with ENSIMAG).

Recherche

Laboratoire : Laboratoire Jean Kuntzmann (LJK)
URL laboratoire : https://ljk.imag.fr
Contact
Prénom/Nom : Clément Pernet et Jean-Guillaume Dumas
Mail : Clement.Pernet@univ-grenoble-alpes.fr et Jean-Guillaume.Dumas@univ-grenoble-alpes.fr
Tél: 04 57 42 17 97 et 04 57 42 17 32

Descriptif recherche:
Contexte et motivations
La sécurité informatique est une discipline scientifique à la croisée des mathématiques et de l'informatique. Elle revêt désormais une importance centrale dans notre quotidien : respect de la vie privée, fuite de données personnelles et espionnage économique, infection de systèmes informatiques sensibles, usurpation d'identité, etc.
La sécurité devient également indispensable pour les problématiques du calcul. D'une part en termes de fiabilité, pour pallier les défaillances liées à l'utilisation d'infrastructures de calcul distribuées par l'utilisation de techniques de tolérance aux fautes. D'autre part dans le contexte où ces infrastructures sont toujours plus externalisées, la problématique de la sécurité des données et des calculs devient centrale. Ainsi, par exemple, les calculs répartis sur ressources non sûres (*cloud, volunteer computing, blockchains*) nécessitent de considérer autant les problématiques de protection des données et de l'anonymat que celles de la fiabilité et de la résilience de ces calculs. Dans ce contexte, l'expertise en informatique mathématique (cryptologie, théorie des codes, calcul algébrique) est devenue essentielle dans le développement de nouvelles applications, telles que la tolérance aux fautes, la cryptographie post-quantique, ou les protocoles d'architecture de sécurité distribuée par chaînes de blocs.
Ces recherches à l'interface des mathématiques et de l'informatique s'étendent de la programmation bas niveau à la théorie des nombres, en passant par l'algorithmique, le calcul ou la complexité. Dans ce domaine, le LJK a développé une forte activité dans trois domaines complémentaires : les protocoles pour la sécurité des calculs externalisés (certification, preuve de récupérabilité, calcul multipartite ou tolérance aux fautes) et embarqués (masquage), la cryptographie (primitives symétriques, cryptologie asymétrique, homomorphe, ou à base de codes), le calcul formel ou algébrique (algèbre linéaire, calcul haute performance, théorie des codes appliquée). Ces travaux s'inscrivent dans des collaborations interdisciplinaires avec de multiples acteurs locaux au sein du *Grenoble Alpes Cybersecurity Institute.*

Description des axes de recherche associés au poste
Le laboratoire Jean Kuntzmann souhaite recruter un(e) maître(sse) de conférences en Cybersécurité et sécurité du calcul dont les activités de recherche relèvent de l'un ou plusieurs des domaines suivants :
— sécurité et fiabilité des calculs distribués ou externalisés, informatique de confiance ;
— protocoles de sécurité, calcul multipartite, protection de la vie privée, anonymat ;
— architectures de sécurité, PKI, blockchain ;
— calcul exact, calcul formel, calcul algébrique ;
— cryptographie et théorie des codes ;
et leurs applications.

Research profile: (version anglaise obligatoire)

Context and motivations

Computer security is a scientific discipline at the crossroads of mathematics and computer science. It is now a central issue in our daily lives: privacy, personal data leakage and economic espionage, infection of sensitive computer systems, identity theft, etc.

Security is also becoming essential for computing issues. On the one hand, in terms of reliability, to compensate for failures linked to the use of distributed computing infrastructures through the use of fault tolerance techniques. On the other hand, in the context where these infrastructures are increasingly outsourced, the issue of data and calculation security becomes central. For example, distributed computing on non-secure resources (cloud, volunteer computing, blockchains) requires consideration of the issues of data protection and anonymity as well as the reliability and resilience of these calculations. In this context, expertise in mathematical computing (cryptology, code theory, algebraic computation) has become essential in the development of new applications, such as fault tolerance, post-quantum cryptography, or blockchain-based distributed security architecture protocols.

This research at the interface of mathematics and computer science ranges from low-level programming to number theory, via algorithmics, computation and complexity. In this field, the LJK has developed a strong activity in three complementary domains: protocols for the security of externalized (certification, proof of recoverability, multiparty or fault-tolerant computing) and embedded (masking) computations, cryptography (symmetric primitives, asymmetric, homomorphic, or code-based cryptography), symbolic or algebraic computation (linear algebra, high-performance computation, applied code theory). This work is part of interdisciplinary collaborations with multiple local actors within the Grenoble Alpes Cybersecurity Institute.

Description of the research areas associated with the position

The Jean Kuntzmann laboratory is seeking to recruit a lecturer in Cybersecurity and Computational Security whose research activities fall within one or more of the following areas:

- security and reliability of distributed or outsourced computing, trusted computing;
- security protocols, multiparty computing, privacy protection, anonymity;
- security architectures, PKI, blockchain;
- exact computation, symbolic computation, algebraic computation;
- cryptography and code theory;

and their applications.

Autres activités collectives

A indiquer en français
La personne recrutée prendra part aux responsabilités administratives de la composante et du laboratoire d'accueil dans le cadre de l'enseignement et de la recherche.

A indiquer en anglais
The hired candidate will participate in administrative responsibilities relative to both teaching and research.

Informations à destination des candidats

- L'Université Grenoble Alpes recrute sur les compétences et fait travailler tous les talents. Elle encourage les candidats en situation de handicap à accéder aux emplois d'enseignants-chercheurs.

- Les enseignants-chercheurs sont astreints à résider au lieu d'exercice de leurs fonctions (l'Art .5 du décret n° 84-431 du 6 juin 1984)