Ingénieur de recherche: Software for rewriting non-commutative polynomials and for proving cryptographic protocols

---

Description du Cluster d'excellence CPU (IdEx – université de Bordeaux)

Les technologies numériques et digitales sont omniprésentes dans notre vie quotidienne et leur utilisation dans les mondes scientifique et industriel évolue sans cesse. Les calculs numériques ont d'abord été utilisés comme un outil pour expliquer les phénomènes complexes pour lesquels des calculs explicites ou des expériences directes n'étaient pas possibles. L'étape suivante a été l'usage du calcul scientifique en tant qu'outil de dimensionnement et de conception dans certains secteurs industriels.

L'idée d'utiliser le calcul scientifique comme outil de certification ou tout au moins comme outil de qualification devient progressivement de plus en plus sensée, non seulement parce que la puissance des ordinateurs augmente sans cesse, mais aussi grâce aux méthodes et aux modèles mis au point aux cours des dernières décennies. Afin d'aborder les problèmes dans le domaine de la certification ou de la qualification, il est nécessaire d'associer plusieurs domaines de la science : la modélisation mathématique et mécanique, l'analyse numérique et l'informatique. L'utilisation de plusieurs milliers de processeurs est inutile sans méthodes numériques fiables, ou avec des modèles imprécis.

A Bordeaux, une masse critique de chercheurs travaille actuellement sur ces sujets, tant du point de vue théorique que de celui des applications, dans le cadre d'un processus interdisciplinaire déjà établi.

L'objectif de ce projet est facile à formuler : nous voulons développer des sciences numériques à un niveau tel qu'elles puissent être utilisées en tant qu'outil de certification.

Plus d'information sur : http://cpu.labex-u-bordeaux.fr/

Durée : 1 an
Type de poste : Ingénieur de recherche temps plein
Lieu: LaBRI/IMB
Date: Le démarrage peut avoir lieu entre le 01/05/15 et le 30/06/15 (suivant les souhaits du candidat).
Rémunération: selon profil et expérience

Description du projet et activités

Description du poste:

CPU
351, Cours de la libération
33405 Talence France
T: 33 (0)540002128
thierry.colin@u-bordeaux.fr / anne-lise.bue@u-bordeaux.fr

Développer le prototype LALBLC qui est un prouveur automatique d'égalités de langages formels,c.f. :
- [P. Henry et G. Sénizergues, CIAA13],
-http://dept-info.labri.u-bordeaux.fr/~ges/LALBLC/lalblc.html
La programmation se ferait en Python, en utilisant SAGE.

Missions de maintenance (20 % du temps):
- écrire le manuel de l'utilisateur
- écrire une documentation du programme
- compléter les modules de test
- améliorer le module de supervision
- installer le programme sous git (gestionnaire de versions).

Missions de recherche et développement (80 % du temps) :
- intégrer le module écrit par les cryptologues Cortier-Delaune-Chretien en 2014
- créer un module qui implémente les algorithmes classiques de réécriture de polynômes non-commutatifs
- créer un module qui implémente des traductions automates finis <–> polynômes non-commutatifs<–> termes
- créer un module qui produise aléatoirement des paires de grammaires équivalentes
- créer un module qui produise des preuves dans un système (G-EQ) plus élémentaire que celui utilisé actuellement puis au format DEDUKTI (concu par INRIA-Roquencourt)
- créer un module de visualisation

Profil du candidat

Compétences demandées :
- solides connaissances en Informatique ET en Mathématiques (masters des deux spécialités)
- expérience de la programmation
- expérience de la gestion de projet
- connaissances en logique et en langages formels
- lecture de l'anglais scientifique

Superviseurs/Contact

Porteurs du projet : G. Sénizergues/G. Zemor

Les dossiers de candidature, constitués d'un curriculum vitae et d'une lettre de motivation doivent parvenir, avant le 10 Avril 2015 inclus à :

Géraud Sénizergues : ges@labri.fr

CPU
351, Cours de la libération
33405 Talence France
T: 33 (0)540002128
thierry.colin@u-bordeaux.fr / anne-lise.bue@u-bordeaux.fr