UNIVERSITE D'ORLEANS

AVIS DE SOUTENANCE EN VUE DE

L'HABILITATION A DIRIGER DES RECHERCHES

Discipline : Informatique

CIUCANU Radu - MCF

présentera ses travaux en vue de l'habilitation à diriger des recherches

Le mercredi 9 juin à 15h

Lieu : Visio Zoom INSA CVL/ LIFO

devant le jury constitué par les personnalités suivantes :

- Nicolas Anciaux, Directeur de Recherches, Inria Saclay-Île-de-France
- Sébastien Gambs, Professeur, Université du Québec à Montreal
- Marie-Christine Rousset, Professeure, Université Grenoble-Alpes
- Sara Bouchenak, Professeure, INSA de Lyon
- Claude Castelluccia, Directeur de Recherches, Inria Rhône-Alpes
- Pascal Lafourcade, Maître de Conférences, HDR, Université de Clermont-Auvergne
- Benjamin Nguyen, Professeur, INSA Centre Val de Loire

Résumé des travaux :

Le but de ce document est de résumer mes activités de recherche depuis mon recrutement en tant que Maître de Conférences en 2016. La plupart de mes recherches pendant cette période ont été consacrées aux problèmes de sécurité des données qui apparaissent lors de l'externalisation des données dans le cloud, suivie par certains calculs (tels que l'évaluation d'une requête ou d'un algorithme d'apprentissage automatique) directement dans le cloud. Je me suis concentré sur le modèle de cloud honnête-mais-curieux, c'est-à-dire qui exécute les tâches consciencieusement, mais essaie d'apprendre le plus d'informations possible. J'ai contribué à: (i) l'évaluation sécurisée de requêtes SPARQL sur des graphes externalisés, et sur la génération synthétique de graphes et requêtes; (ii) des protocoles sécurisés pour les algorithmes d'apprentissage automatique séquentiel, en mettant l'accent sur les bandits; (iii) des protocoles MapReduce sécurisés pour le produit matriciel et l'évaluation des requêtes relationnelles. Notre approche consiste à développer des protocoles distribués et sécurisés qui combinent des algorithmes existants avec des techniques cryptographiques (telles que AES et Paillier) et du calcul multipartite sécurisé. Nos protocoles garantissent le même résultat que les algorithmes standard non-sécurisés tout en bénéficiant de propriétés de sécurité.