

# Sujet de stage de M2 recherche

## Modélisation et calcul de la capacité des canaux cachés

Catalin Dima, [dima@u-pec.fr](mailto:dima@u-pec.fr)  
LACL, Université Paris Est Créteil, 61 av. du Général de Gaulle, 94010 Créteil Cedex,

### Contexte

Les canaux cachés sont des canaux de communication entre des sujets se trouvant dans des niveaux de sécurité différents, qui utilisent des moyens de communication légale pour se transmettre des informations sensibles. Par le caractère légal de la communication, les canaux cachés ne sont pas détectables, mais on peut quantifier leur menace par leur débit – ou capacité. Une analyse de sécurité d’un système doit être capable de détecter les canaux cachés dans le système et d’approximer leur capacité.

Nous avons proposé dans [1] une approche de modélisation des canaux cachés (non-probabilistes et unidirectionnels) par des transducteurs finis, et de définir la capacité d’un canal caché d’une manière similaire à l’entropie d’un automate fini.

Nous avons étudié une série de techniques d’approximation de la capacité des canaux cachés, dont certaines basées sur le calcul des (approximations des) rayons spectraux communs (angl. *joint spectral radius*). Le problème du calcul “exact” de la capacité d’un canal caché reste encore ouvert – dans le sens de la possibilité de décrire la capacité d’un canal caché comme, par exemple, la plus grande solution positive d’un polynôme de coefficients entiers construit algorithmiquement à partir du transducteur modélisant le canal.

Ces travaux seront poursuivis dans le cadre du nouveau projet de recherche ANR “EQINOCS” (Entropy and Quantity of Information in models Of Computational Systems) qui se propose d’adapter et d’appliquer la notion d’*entropie* aux modèles de systèmes computationnels.

### Objectifs du stage

Le stagiaire participera aux travaux théoriques, au sein du projet EQINOCS, sur l’identification de meilleures techniques d’approximation ou de calcul exact de la capacité des canaux cachés modélisés en transducteurs finis. Un autre aspect du travail envisagé sera d’implémenter les algorithmes obtenus et d’évaluer leur efficacité sur des modèles de canaux cachés.

### Financement, poursuite en thèse

Le stage est financé sur le projet EQINOCS, et les travaux pourront être poursuivis dans le cadre d’une thèse en co-tutelle LACL (UPEC) – LIGM (Univ. Marne-la-Vallée), financée sur le même projet de recherche.

### Compétences souhaitées et modalités de candidature

Le candidat idéal devrait avoir de bonnes bases en théorie des automates et algèbre linéaire, et une ouverture pour la recherche théorique en informatique.

Pour candidater, contacter Catalin Dima ([dima@u-pec.fr](mailto:dima@u-pec.fr)), en envoyant un résumé des relevés de notes.

### Information équipe de recherche

Équipe *Spécification et vérification des systèmes*, Laboratoire d’Algorithmique, Complexité et Logique (LACL), directeur Régine Laleau, [mél.laleau@u-pec.fr](mailto:mél.laleau@u-pec.fr).

### Références

1. E. Asarin and C. Dima. On the computation of covert channel capacity, *RAIRO - Informatique Théorique et Applications*, vol. 44, p. 37-58, 2010. Version en ligne : <http://lacl.univ-paris12.fr/dima/work/covertchannels.pdf>.