

# Architecture de sécurité pour systèmes multiprocesseurs intégrés sur puce

## Mots clés :

- **Directeur de thèse** : Alain Greiner
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

## Résumé du projet de recherche (Langue 1)

Le co-hébergement sécurisé de piles logicielles autonomes sur systèmes multiprocesseurs intégrés sur puce est un sujet d'actualité. Dans le marché des produits (puces) orientés multimédia, ces piles logicielles autonomes représentent généralement les intérêts des différentes parties prenantes. Ces parties prenantes sont multiples (fabricants, fournisseur d'accès, fournisseurs de contenus, etc.) et ne se font pas forcément confiance entre elles, d'où la nécessité de trouver une manière de les exécuter ensemble mais avec certaines garanties d'isolation. Les ressources de calcul -- processeurs -- des puces multimédia étant fortement hétérogènes -- peu de processeurs généralistes sont assistés par une multitude de processeurs ou coprocesseurs spécialisés -- et à mémoire partagée, il est difficile voire impossible de résoudre cette problématique en utilisant une unique base de confiance, comme le préconise les récentes techniques de virtualisation. Le travail de thèse a donc consisté à définir un nouveau modèle de confiance plus flexible et générique que l'existant, qui permet à ces piles logicielles de s'exécuter simultanément sur ces plateformes matérielles non-homogènes. Dans la même optique, nous avons étudié et proposé des solutions pour le partage des périphériques entre ces piles logicielles, notamment concernant les périphériques ayant une capacité DMA beaucoup utilisés dans les systèmes orientés multimédia ; cette étude sur le partage des périphériques s'est également intéressé au problème de redirection des interruptions matérielles. Enfin, la réalisation de certains morceaux choisis du modèle proposé a permis de valider l'approche de principe, mais surtout d'en mesurer l'éventuel surcoût, en terme de performance et de surface matérielle.