Avis de Soutenance

Monsieur Paul-Antoine MATRANGOLO

Electronique, Micro et Nanoélectronique, optique et laser

Soutiendra publiquement ses travaux de thèse intitulés

Processeur Sécurisé et Reconfigurable Incluant des Technologies Émergentes

dirigés par Monsieur David NAVARRO

Soutenance prévue le ***jeudi 17 avril 2025*** à 10h00
Lieu : INL Campus de la Doua 3 Rue Enrico Fermi, 69100 Villeurbanne
Salle : bâtiment IJC, des thèses

Composition du jury proposé

M. David NAVARRO	Ecole Centrale de Lyon	Directeur de thèse
Mme Ioana VATAJELU	Laboratoire TIMA	Rapporteure
M. Jean-Michel PORTAL	Université Aix-Marseille	Rapporteur
M. Cédric MARCHAND	Ecole Centrale de Lyon	Co-encadrant de thèse
M. Damien DELERUYELLE	Institut National des Sciences Appliquées	Examinateur
M. Jean-François DAYEN	Université de Strasbourg	Examinateur

Mots-clés : sécurité,technologies émergentes,calcul en mémoire,,

Résumé :

L'Internet des Objets, raccourcie en IoT pour Internet of Things, est un écosystème en pleine expansion, où des objets intelligents interagissent via des réseaux communicants. Cette croissance rapide entraîne une augmentation massive des données collectées, posant des défis en termes d'efficacité énergétique, notamment au niveau des nœuds de capteurs. Pour améliorer cette efficacité, il est essentiel de traiter les données au plus près des capteurs, ce qui réduit la charge de communication et d'opérations sur l'unité de calcul principale. L'approche du Near Sensor Computing et l'utilisation de mémoires non volatiles (NV), capables de maintenir l'état des capteurs en veille, permettent de répondre à ces défis tout en augmentant significativement l'efficacité énergétique des systèmes liés à l'IoT. Parallèlement à ces défis énergétiques, la sécurité des données dans l'IoT est devenue une préoccupation majeure, notamment pour des applications où la sécurité est un aspect primordiale comme les véhicules connectés et les systèmes de santé intelligents. Des attaques sur les communications sécurisées ont démontré la vulnérabilité des systèmes actuels face à des menaces sophistiquées. Ainsi, la protection des données dès leur collecte, avant même qu'elles ne soient transmises, est cruciale. Le projet SECRET tente de répondre à ce besoin en appliquant des paradigmes de calcul centrés sur la mémoire et en intégrant des opérateurs reconfigurables et NV au plus près des capteurs. Offrant ainsi une première ligne de défense tout en optimisant la consommation énergétique grâce à la réduction des accès mémoire. L'émergence de technologies émergentes, telles que les transistors à effet de champ ferroélectriques (FeFET) et les mémoires résistives (RRAM), ouvre des perspectives prometteuses pour la conception de circuits basés sur des architectures centrées sur la mémoire. Ces approches, en rupture avec les architectures de Von Neumann ou Harvard, permettent de limiter les goulots d'étranglement liés aux transferts de données entre unités de calcul et de stockage. Cependant, leur intégration dans des circuits complexes soulève plusieurs défis techniques majeurs. D'une part, le choix des modèles doit être judicieux afin d'assurer la précision des simulations et la fiabilité des résultats tout au long du flot de conception. D'autre part, les outils de conception actuels, principalement développés pour des architectures conventionnelles, sont encore peu adaptés aux spécificités des circuits exploitant un effet mémoire intrinsèque. En particulier, la prise en compte des propriétés NV des composants et leur impact sur la synthèse logique nécessitent des méthodologies adaptées. Cette thèse montre qu'il est possible de concevoir des portes logiques basées sur des FeFET puis propose une application au sein d'opérateurs NV.