# ACTIVITES DE RECHERCHE :

*(Présentation des thématiques de recherche : grands axes de recherches et apport dans le ou les domaines concernés*)

*L'axe principal, qui a dominé mes activités de recherche ces dernières années, concerne l'optimisation des architectures reconfigurables de type FPGA, en étudiant plusieurs topologies du réseau d'interconnexion. Ce réseau est classiquement de type matriciel (Mesh). Nous avons élaboré des réseaux plus performants de types arborescents (Tree) ainsi qu'un mélange entre ces deux types de réseaux. Pour pouvoir bien explorer ces architectures, nous avons également développé les outils de partitionnement, de placement et de routage associés. L'ensemble de ces activités ont permis la conduite d'une douzaine de thèses de doctorat, de plus de 80 publications internationales dans les conférences et revues, deux brevets, deux livres et une startup. Ces recherches n'auraient pu être conduites sans les rayonnements académiques et industriels qui ont permis de générer un nombre de projets et de contrats.*

*En parallèle à ces travaux, je me suis également intéressé à la sécurisation des architectures FPGA contre les attaques en canaux cachés et naturellement à développer des recherches sur les architectures pour la cryptographie.*

*Dans cette présentation, je vais décrire celles de ces cinq dernières années et qui sont en cours ou récemment achevées.*

## THEME I : ARCHITECTURES RECONFIGURABLES A GRAINS VARIABLES POUR LES SYSTEMES SUR PUCE

***Thèses achevées de Umer FAROOK et de Husain PARVEZ (CEA-DAM)***

*Les circuits programmables de type FPGA présentent un compromis très intéressant entre la souplesse du logiciel et de la performance du matériel. Toutefois, ces types de circuits, comparativement aux ASICs dédiés, présentent, en moyenne, une surface 40 fois plus grande, une vitesse 4 fois plus faible et une consommation 12 fois plus importante.*

*Les FPGAs classiques sont constitués, typiquement, par des blocs logiques implantés sous formes de tables de vérité (LUT) et d'un réseau d'interconnexion liant ces blocs. Afin d'améliorer les performances des FPGAs, en termes de surface, vitesse et consommation, l'architecture de base de ces FPGAs est modifié par l'insertion de blocs complexes (gros grains) comme des multiplicateurs, additionneurs, RAMS, etc. Ces circuits deviennent, alors, à grains variables.*

*En parallèle de ce travail d'architectures, on a développé une plateforme d'exploration d'espaces de solutions de placement optimisé des blocs reconfigurables (grains fins et gros grains) en tenant compte, également de la projection de netlist et de son routage.*

## THEME II :ARCHITECTURES FPGA EMBARQUEES SECURISEES CONTRE LES ATTAQUES DPA

***Projet SeFPGA ANR ARFU2007 (Secure embedded FPGA)***
***En partenariat avec TELECOM-Paris***
***Thèse achevée d'Emna AMOURI***

*Le projet SeFPGA vise à étudier la sécurisation des FPGAs personnalisés embarquant des cryptoprocesseurs. Le but est de mettre en œuvre des contre-mesures face aux attaques par canaux cachés ou par injection de fautes. Les protections sont étudiées à la fois au niveau de l'architecture intrinsèque du FPGA et au niveau application. Les architectures FPGAs considérées sont de types matricielles (structure classique) et arborescentes. La sécurisation au niveau application consiste à ajuster le degré de robustesse à tous les niveaux du flot de conception de façon à obtenir la meilleure répartition entre la complexité et la sécurité du FPGA.*

*Au niveau de notre laboratoire, l'objectif de ce travail est de développer les outils du flot de configuration permettant de sécuriser les architectures FPGA, contre les attaques de type DPA « Differential Power Analysis ».*

**THEME III :RECEPTEUR RADIO LOGICIELLE BASE SUR UN DSP RECONFIGURABLE**
***Projet ASTECAS***
***ANR BLANC INTERNATIONAL EDITION 2009***

***Thèse récemment achevée d'Alp KILIC***

L'un des avantages les plus importants d'une structure FPGA est sa capacité à être reconfigurée à la volée. L'idée principale de ce projet est d'utiliser une architecture dynamique reconfigurable à base de circuit FPGA pour traiter différents multistandards de télécommunications. Pour ne pas accroitre la complexité du projet, on cherchera à implanter les normes suivantes : Bluetooth, Zigbee et WiFi.
L'architecture du système sur puce adoptée sera composée de blocs :RF, analogique et numérique. Ce dernier sera réalisé par la partie reconfigurable qui sera embarqué sur la puce.
Pour réaliser les différents blocs ainsi que l'ensemble du système, on utilisera une modélisation SystemC-AMS. Pour optimiser la partie reconfigurable, on bénéficiera de travaux antérieurs sur la conception de circuits FPGA spécifiques.

**THEME IV: SYNTHESE D'ARCHITECTURES DE FPGA TOLERANT AUX DEFAUTS**
Projet ROBUST FPGA
***ANR INS 2011***
Doctorant: Adrien BLANCHARDON
Thèse co-encadrée avec Roselyne Chotin-Avot, Maître de Conférences.

Les travaux de recherche effectués dans cette thèse permettront de proposer une IP de FPGA tolérante aux défauts.

L'équipe CIAN du LIP6 développe depuis quelques années un environnement de conception de circuits numériques : Stratus. Cet environnement a déjà permis de développer différentes architectures reconfigurables de type FPGA avec une topologie matricielle ou arborescente.

L'objectif de cette thèse est d'étudier et de développer une IP de FPGA de robustesse accrue contrôlée au niveau architectural (interconnexion et logique), intégrable seule ou pouvant être embarquée.

Au sein de cette IP, la robustesse sera intégrée au niveau architectural :

- dans les éléments logiques et les blocs d'interconnexion critiques afin de les rendre plus robustes
- dans le réseau d'interconnexion en permettant le contours des ressources défectueuses
- dans l'architecture générale en insérant des mécanismes de test et de diagnostic permettant de générer la cartographie des défauts présents dans le circuit.

L'essor considérable de la technologie CMOS a permis l'accroissement de la densité d'intégration selon la loi de Moore. Cependant, la poursuite de cette évolution est en voie de ralentissement dû aux contraintes physiques et économiques. En particulier, une réduction importante des rendements de fabrication des systèmes sur puce (SoC) est observée. Elle s'accompagne de coûts de fabrication très importants.

Ce changement induit un bouleversement des pratiques de conception. Les concepteurs ne doivent plus raisonner en termes de circuits seulement bons ou mauvais après test de production. Le défi

devient alors de pouvoir utiliser un maximum de circuits tout en tolérant des défauts physiques présents en leur sein.

**THEME V : ARCHITECTURES MATERIELLES POUR LA CRYPTOGRAPHIE**
Doctorant: **Karim MOUSSA ALI ABDELLATIF**
Thèse co-encadrée avec Roselyne Chotin-Avot, Maître de Conférences.

Les travaux de recherche effectués dans cette thèse conduiront, dans une première étape, à la conception d'une bibliothèque d'opérateurs arithmétiques génériques dédiés à la cryptographie puis, dans une seconde étape, à l'étude d'un système sur puce (SoC) permettant le cryptage/décryptage de données.

Le développement de l'internet fixe ou mobile, confère une place importante aux systèmes d'information qui véhiculent au quotidien les données numériques échangées sur l'ensemble de la planète. L'enjeu de la sécurisation des données est donc au cœur des préoccupations des concepteurs de systèmes d'information. La cryptographie s'intéresse uniquement à la protection des messages en assurant la confidentialité et l'authenticité des communications. Il existe de nombreux algorithmes de cryptographie permettant la protection des données. Ces algorithmes, pour être fiables, nécessitent d'importants calculs et il est inenvisageable de les intégrer directement dans un système embarqué. C'est pourquoi, dans le cadre de cette thèse, nous envisageons de concevoir un système sur puce qui permettrait de crypter/décrypter à la volée les données. Les algorithmes de cryptographie à clé publique nécessitent des opérateurs en arithmétique modulaire ou des opérateurs sur les corps finis. Une première étape de la thèse sera donc de proposer des architectures pour ces opérateurs adaptés à la cryptographie à clé publique. Ensuite ces opérateurs seront utilisés pour la conception d'un coprocesseur de cryptographie qui sera intégré dans un système sur puce. Pour la conception matérielle du coprocesseur, l'étude profitera amplement des recherches effectuées dans l'équipe Circuit Intégrés Analogiques Numériques (CIAN) concernant notamment le développement d'une bibliothèque riche de composants arithmétiques de base et l'expertise en terme d'adéquation algorithme architecture. Pour l'intégration du coprocesseur dans un système sur puce, on profitera des recherches menées par l'équipe « Architectures et Logiciels pour les systèmes intégrés sur puce » (ALSoC) autour du projet SocLib avec le développement d'une bibliothèque de modèles de simulation de composants matériels et l'environnement de conception conjointe matériel/logiciel DSX.

**THEME VI: ARCHITECTURE FPGA UTILISANT LA TECHNOLOGIE 3D**

Doctorant: **Vinod PANGRACIOUS**

Les réseaux programmablex (FPGA) deviennent des acteurs importants dans le domaine de l'architecture qui a été à l'origine dominé par les microprocesseurs et les ASIC. Le grand défi des circuits FPGA est de trouver un bon compromis entre la flexibilité et les performances. Trois facteurs se combinent pour déterminer les caractéristiques d'un FPGA: la qualité de son architecture, la qualité des outils de CAO utilisés pour mapper des circuits dans le FPGA, et sa conception dans la technologie cible. Ce projet de recherche vise à explorer une méthodologie de développement de l'architecture FPGA dans une technologie 3D pour améliorer la superficie, la densité, la consommation d'énergie et les performances temporelles.

**THEME VII : TECHNIQUES DE MULTIPLEXAGE POUR UN SYSTEME D'EMULATION ET DE PROTOTYPAGE RAPIDE A BASE DE CIRCUITS FPGA.**

Thèse co-encadrée avec Zied Marrakchi, chercheur.
Doctorant: **Mariem TURKI**
Sujet de thèse en cotutelle Directeur de thèse du coté Français : Habib MEHREZ (PR LIP6-UPMC)
Co-encadrant du coté Français : Zied MARRAKCHI (ex-Docteur LIP6-UPMC)

Avec la tendance mondiale vers le numérique, la complexité de la conception de circuits intégrés et du logiciel croit régulièrement tandis que la durée de vie des circuits et des produits se réduit. La vérification est une étape importante pour la création du produit final et c'est une composante clé pour la réussite de la commercialisation dans les délais prévus. Avant de produire le silicium réel, il n'y a que trois possibilités de vérification : un prototype sur FPGA, une simulation et une émulation. Le prototypage matériel présente le meilleur compromis entre le temps de conception d'un circuit et le temps d'exécution d'une application sur ce circuit. Une plateforme de prototypage propose une carte multi-FPGA et un flot logiciel assurant l'implantation du circuit à vérifier sur la carte. En général, les circuits complexes à développer dépassent la capacité logique d'un seul FPGA, d'où la nécessité de les découper sur différents FPGA (partitionnement). La manière dont le circuit est découpé a un effet très important sur les performances et le comportement du système de prototypage. L'outil de partitionnement permet d'obtenir une répartition du circuit objet du prototypage sur les FPGA de la carte. Cette répartition tente de tirer le meilleur profit de l'architecture du FPGA en tenant compte des contraintes imposées par celle-ci en termes de surface disponible (portes logiques). Son objectif est de minimiser les chaînes longues de manière à obtenir la performance la plus élevée en termes de fréquence de fonctionnement. Toutefois, compte tenu de la complexité des circuits à partitionner, toutes les contraintes ne peuvent pas être satisfaites par cet outil. En effet, les FPGA disposent d'un nombre limité de ressources d'entrée-sortie. Or, a priori, cette ressource matérielle détermine le nombre de signaux qui peuvent apparaître à l'interface de deux parties et qui doivent passer d'un FPGA à un autre. Les contraintes imposées par la limitation de cette ressource sont telles qu'il se peut qu'aucune partition réaliste ne puisse les satisfaire. Dans cette étude, nous proposons de développer un outil spécifique qui intervient après le partitionnement pour prendre en compte la contrainte liée à la limitation du nombre de fils d'interconnexion entre deux FPGA. Cette thématique demande la synergie entre plusieurs compétences complémentaires : Spécifications de cartes électroniques multi-FPGAs, conception de circuits intégrés à vérifier et développement d'outil d'optimisation CAO. Il en résulte l'utilité de réaliser une coopération entre une équipe spécialisée surtout en conception de circuits intégrés et cartes électroniques (équipe tunisienne) et une équipe spécialisée surtout en informatique dans les techniques algorithmiques d'optimisation VLSI (équipe française).

## ENCADREMENT ET ANIMATION DE LA RECHERCHE :

- ***Direction, animation laboratoires et équipes de recherche***

*Depuis avril 2008, je suis responsable de l'équipe CIAN (Circuits Intégrés Analogiques et Numériques) du LIP6 (http://www.lip6.fr/recherche/team.php?id=940). Cette équipe se compose en moyenne d'environ 30 personnes et mène des activités autour de quatre axes principaux :*

1) *Fonctions analogiques multi contextes*
2) *Architectures numériques et reconfigurables*
3) *Plateforme Coriolis (plateforme Open source pour la conception des circuits intégrés)*
4) *Outils de vérification bas niveau (backend)*

- ***Organisation colloques, conférences, journées d'étude***

*Membre de comités de lecture de plusieurs conférences et revues nationales et internationales (ACM, DETIS, SETIT et Microelectronics jounal).*

- ***Direction de thèses et autres travaux***

*Direction de 30 thèses d'universités soutenues (détail en annexe).*
*Pour les cinq dernières années, les thèses soutenues sont synthétisées dans le tableau suivant :*

| *Nom doctorant* | *Sujet* | *projet* | *1ère inscription* | *Fin* | *Taux encadrement* |
|---|---|---|---|---|---|
| *Umer FAROOQ* | "Exploration and optimization of application specific heterogeneous tree-based FPGA architectures". | *CEA-DAM* | *Septembre 2008* | *Juillet 2011* | *100%* |
| *Emna AMOURI* | "Outils de placement et de routage pour des architectures FPGA sécurisées contre les attaques DPA". | *SeFPGA (Secure FPGA)* | *Septembre 2008* | *Septembre 2011* | *100%* |
| *Alp KILIC* | "Méthodologie d'optimisation d'architectures pour les applications mutuellement exclusives" | *ASTEC AS Radio logicielle* | *Septembre 2009* | *18 nov 2013* | *100%* |
| *Mariem TURKI* | Techniques de multiplexage pour un système d'émulation et de prototypage rapide à base de circuits FPGA | *Systematic-FEDER Projet PPR* | *2011-2012* | *17 septembre 2014* | *50%* |
| Karim MOUSSA ALI ABDELLATIF | Architectures matérielles pour la cryptographie | *CEA-DAM* | *2011-2012* | *7 oct 2014* | *20%* |
| Vinod PANGRACIOUS | Architecture FPGA Utilisant la technologie 3D | *LIP6-CIAN* | *2011-2012* | *24 nov 2014* | *50%* |
| Jung Kyu CHAE | Un Environnement Logiciel Global pour le développement et la validation d'une plateforme de concpetion | CIFRE ST | *2011-2012* | *8 Juillet 2014* | *50%* |
| Boukary OUATTARA | Prévision des effets de vieillissement par électromigration dans des bibliothèques et les systèmes sur puces CMOS | *CIFRE ST* | *2011-2012* | *9 Juillet 2014* | *50%* |
| Qingshan TANG | Méthodologies de Génération Automatique de Plateforme de Prototypage sur Mesure pour Systèmes Embarqués | *CIFRE FLEXRAS* | *2011-2012* | *Décembre 2014* | *100%* |
| Adrien BLANCHARDON | Synthèse d'architectures DE FPGA tolérant aux défauts | ROBUST FPGA ANR INS 2011 | 2011-2012 | Juillet 2015 | 20% |

***Contrats de recherche***

*Le tableau précédent indique l'association des travaux de thèse à différents contrats de recherche de type ANR ou pôle de compétitivité System@tic ( ASTECAS, RobustFPGA, SeFPGA et PPR). J'ai monté également des projets industriels (STmicroelectronics et FlexRas) ainsi que publiques avec le CEA-DAM,*

*J'ai également monté un nouveau projet de plateforme de prototypage rapide Multi-FPGA (projet Wasga Server) dans le cadre de FUI18. Ce projet réunit le consortium suivant : Bull, CEA-LIST, RefLex et le LIP6. Ce projet est en cours et s'achèvera en avril 2018.*
*Dans ce cadre, j'assure l'encadrement de 3 post-doc*

***Réseaux de recherche***

*Création de réseaux de recherche avec notamment des universités brésiliennes (accords CAPES-COFECUB) et des universités tunisiennes (accords CMCU et CNRS-DGRSRT).*

***Valorisation de la recherche** :*

*- Contribution récente à la création d'une deuxième startup (FlexRas pour Flexible Reconfigurable Architectures and Software) pour valoriser nos travaux sur les architectures FPGA et les outils de configuration associés. Cette startup a été lauréat au concours émergence en 2007 et lauréat en 2009 au concours création.*

*- Dépôt de deux brevets l'un en France et le second aux Etats-Unis sur deux topologies d'interconnexion pour architectures FPGA.*

*- Montage de projets et de contrats avec le CEA-DAM sur mes thèmes de recherche, en moyenne un contrat par an depuis environ 20 ans.*

*- Contrats industriels avec STmicroelectronics et les startups issus du laboratoire.*