Le projet SeFPGA vise à étudier la sécurisation des FPGAs personnalisés embarquant des cryptoprocesseurs. Le but est de mettre en oeuvre 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 arboresentes. 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.

Contact

Jean-Luc DANGER
TELECOM PARISTECH (ENST)
01 45 81 81 17
danger@telecom-paristech.fr

SEFPGA
Secured FPGA

PLAN DU PROJET ET DÉLIVRABLES

0 - Faire part de l'avancement et des résultats par le biais d'un site web
1 - Elaborer un rapport sur la sécurisation au niveau logique pour FPGA
2 - Etudier et concevoir les outils de CAO dédiés au FPGA hiérarchique avec option de sécurité
3 - Etudier et concevoir les outils de CAO dédiés au FPGA Mesh avec option de sécurité
4 - Spécifier et faire le modèle VHDL d'un circuit prototype
5 - Concevoir et tester un circuit ASIC prototype
6 - Faire la synthèse des résultats par le biais de rapports de thèse

PRINCIPALES PHASES DU PROJET

CAO pour la sécurisation au niveau logique
- Etudes des logiques candidates pour la sécurité
- Etudes des compromis sécurité/complexité
- Conception d'un outil de CAO pour la sécurisation de netlists

CAO spécifique au FPGA en arbre
- Partitionnement
- Routage
- Partitionnement sécurisé
- Routage sécurisé dual rail

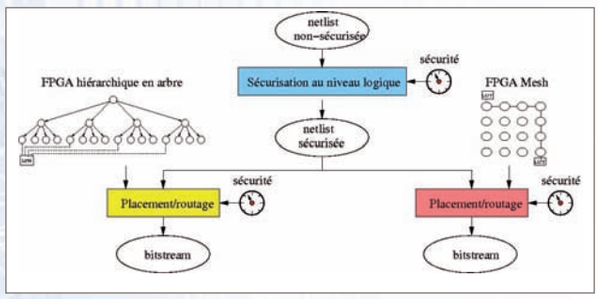
CAO pour la sécurisation spécifique au FPGA en matrice
- Placement sécurisé dual rail
- Routage sécurisé dual rail

Spécification du FPGA en arbre prototype
- Structures logiques et interconnexion sécurisées
- Structure de configuration

Conception d'un circuit prototype
- Génération des masques
- DRC, LVS, STA
- Tape-out

Test du circuit prototype et évaluation de la robustesse
- Conception de la carte de test
- Tests fonctionnels
- Evaluation de la robustesse

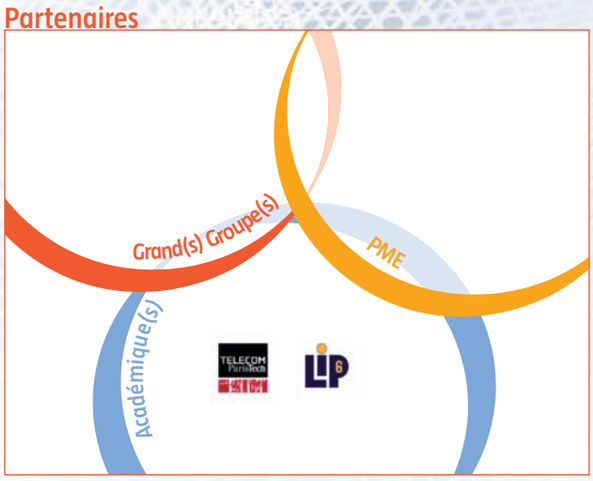
Rapports de thèse
- Rapport sur La sécurisation d'un FPGA Mesh
- Rapport sur la sécurisation d'un FPGA arborescent



STATUT

Réalisation d'un outil de sécurisation de netlist contre la DPA en utilisant la logique WDDL+. sur ALTERA et XILINX.
Première version d'outils de partitionnement et routage du FPGA arborescent

Partenaires



Coordinateur : TELECOM PARISTECH

Partenaires : LIP6, TELECOM PARISTECH, UNIVERSITÉ PIERRE ET MARIE CURIE

Durée : 36 mois

Budget Global : 0,82 M€

Financement : 0,37 M€ - Agence Nationale de la Recherche