

Sujet de stage (NUC-RAD@WORK-01)

NUCLETUDES, pôle numérique

L'entité Rad@Works de NUCLETUDES a pour mission de réaliser des travaux de R&T afin de proposer des techniques innovantes dans le domaine de la vulnérabilité et la tenue de systèmes électroniques aéronautiques et spatiaux dans des conditions environnementales sévères. A ce titre, le développement de techniques améliorant l'observabilité du comportement en environnements sévères de composants est clef pour l'évaluation de la tolérance aux fautes.

C'est dans ce cadre que nous proposons l'offre de stage suivante :

Etude de l'impact des stratégies de protection sur les signatures des attaques par canaux auxiliaires d'un FPGA

Les composants numériques de technologies avancées offrent de nombreuses perspectives d'utilisation pour des applications critiques dans les domaines de l'aérospatial et de la défense. Ces environnements se caractérisent par des contraintes potentiellement fortes (environnement radiatif notamment) sur l'électronique. Pour assurer la tolérance aux fautes des composants électroniques, des stratégies de protection doivent être implémentées mais il est en revanche nécessaire de s'assurer que l'implémentation de ces stratégies n'impacte pas négativement d'autres performances critiques de ces composants notamment, pour certains d'entre eux, leur vulnérabilité d'un point de vue SSI (Sécurité des Systèmes d'Informations).

Le sujet de stage proposé est d'étudier, sur une cible FPGA, l'évolution des signatures vis-à-vis d'attaques par canaux auxiliaires (*side channel attacks*) en fonction de l'implémentation de différentes stratégies de protection vis-à-vis des fautes.

Les travaux seront menés sur une cible FPGA implémentée sur une carte de test déjà instrumentée pour mener des études d'attaques par canaux auxiliaires. L'organisation de ce stage se décomposera ainsi en 4 phases :

- 1) Etude bibliographique afin de s'appropriier les notions liées à la tolérance aux fautes et aux attaques par canaux auxiliaire et prise en main de la carte FPGA instrumentée pour mener ces études
- 2) Implémentation d'un processeur synthétisable (softcore) sur la cible FPGA et mesure des signatures vis-à-vis d'attaques par canaux auxiliaires
- 3) Implémentation de techniques de tolérances aux fautes pour le processeur softcore
- 4) Analyse comparative des signatures vis-à-vis d'attaques par canaux auxiliaires en fonction des techniques de tolérances aux fautes implémentées

Profil du candidat :

Vous êtes en dernière année d'école d'ingénieur ou de master en sciences avec des connaissances en microélectronique numérique, architecture des processeurs et conception de systèmes embarqués et vous envisagez ensuite de poursuivre vos études dans le cadre d'un doctorat.

- ❖ Les compétences (techniques) essentielles pour ce stage sont :
- ❖ Bonne connaissance des langages de description matériel (HDL) et du flot de conception sur FPGA
- ❖ Bonne connaissance des architectures de processeurs
- ❖ Connaissance en instrumentation et mesure électronique
 - Maîtrise des langages de description matérielle (VHDL/Verilog)
 -
 - Maîtrise de conception/simulation FPGA (Vivado, QuestaSim, ..)
 - Maîtrise des langages de programmation (C/C++, Python)
 - Maîtrise de l'anglais technique
 - Utilisation de base de l'instrumentation de laboratoire

- ❖ Les compétences non-essentielles mais toutefois fortes utiles pour ce stage sont :
 - Connaissance sur le fonctionnement des bus de communication (AXI)
 - Connaissance sur le fonctionnement des soft processeurs (RISC-V)
 - MPSoC Zynq AMD et/ou FPGA Polarfire Microchip
 - Forte autonomie et curiosité scientifique

Profil compatible d'une habilitation défense.

Le stage se déroule aux Ulis (91).

Si vous êtes intéressé(e) par cette offre, merci d'adresser votre candidature (cv + lettre de motivation) :

Laëtitia Le Mercier, Directrice des Ressources Humaines et de la Communication

llemercier@nuclétudes.com