APPEL à CONTRIBUTION

Sécurité, fiabilité et test des SoC² : challenges et opportunités dans l'ère de l'Intelligence Artificielle

Date : jeudi 16 mai 2019
Lieu : Paris

Les techniques de *Machine Learning* (ML), notamment basées sur des réseaux neuronaux profonds, ou *Deep Neural Networks* (DNNs), sont largement utilisées pour de nombreuses applications dont la vision par ordinateur, la reconnaissance vocale, la robotique, et aussi dans des applications critiques comme par exemple les véhicules autonomes.
Dans le dernier cas d'application, une attention particulière est donnée à la *robustesse* de l'implémentation matérielle du *Machine Learning*. Cela se traduit par la nécessité de garantir non seulement un certain niveau de **fiabilité** vis à vis des pannes qui peuvent toucher les composants électroniques, mais aussi un ensemble de propriétés de **sécurité** permettant de faire face aux attaques ciblant le composant.
Les techniques de *Machine Learning* ouvrent également de nombreuses perspectives dans le cadre de la détection de comportements anormaux pouvant être causés par des fautes naturelles ou des attaques intentionnelles pouvant elles-mêmes s'appuyer sur ces mêmes techniques.
A travers cette journée thématique, nous souhaitons initier des discussions et des échanges autour des différents problématiques liées à la sécurité, à la fiabilité et au test des implémentations matérielles du *Machine Learning*. De plus, nous envisageons des échanges autour de l'exploitation des techniques de ML dans le contexte de la sécurité (e.g., identification des attaques, nouvelles attaques et protections) de la fiabilité et du test (e.g., détection d'un comportement fautif et contre-mesure). L'objectif est aussi d'échanger autour de dépôts de projets pour les différents appels à venir (ANR, FUI, H2020, etc.).
À l'issue de cette journée, une autre journée thématique sera éventuellement organisée sur des problématiques ciblées dans le courant de l'année 2019 afin de poursuivre les discussions scientifiques et de faire maturer les idées de projets.

Thématiques proposées, mais non limitées :

- Fiabilité et test des implémentations matérielles pour le *Machine Learning*
- *Machine Learning* techniques pour le test and le diagnostique des circuits intégrés
- Approximation et Tolérance aux Fautes des implémentations matérielles pour le M*achine Learning*
- Sécurité des implémentations matérielles pour le *Machine Learning*
- Le M*achine Learning* et la sécurité des composants (attaques, détection et protections)
- ...

Organisateurs :

- Vianney Lapôtre - vianney.lapotre@univ-ubs.fr - Université Bretagne Sud - Lab-STICC
- Alberto Bosio - alberto.bosio@ec-lyon.fr – École Centrale de Lyon - INL

Soumissions:

Les propositions se feront sous la forme d'un titre et d'un résumé de moins d'une dizaine de lignes à envoyer avant le 01 avril 2019 par simple mail aux 2 organisateurs.

Inscriptions:

L'inscription est gratuite mais obligatoire pour des raisons logistiques évidentes.
Vous pouvez d'ores et déjà vous inscrire à cette journée par simple mail aux 2 organisateurs.