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

Compte rendu de journée thématique

Date : 20 Mai 2019

Lieu : Laboratoire LIP6, UPMC, Paris

Organisation et rédaction du compte rendu : Vianney Lapôtre, Alberto Bosio

---

Contexte

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.
Durant cette journée thématique, nous avons échangé autour des différentes problématiques liées à la sécurité, à la fiabilité et au test des implémentations matérielles du Machine Learning. De plus, nous avons abordé l'exploitation des techniques de ML dans le contexte de la sécurité (e.g nouvelles attaques et protections) de la fiabilité et du test (e.g., détection d'un comportement fautif et contre-mesure).

Programme de la journée

- 09h30 - 10h00 : Accueil
- 10h00 - 10h50 : Ioana Vatajelu : "Spiking Neural Networks with STDP"
- 10h50 - 11h20 : Ihsen Alouani : "Could we Trust CNNs for Critical Applications?, A Reliability Study"
- 11h20 - 12h10 : Haralampos Stratigopoulos : "Machine Learning Applications in Semiconductor Manufacturing and Test"
- 12h10 - 13h00 : Repas (plateaux repas sur place)
- 13h00 - 13h30 : Safa Mhamdi : "Towards Improvement of Mission Mode Failure Diagnosis for System-on-Chip"
- 13h30 - 14h20 : Emmanuel Prouff : "Deep Learning against Secure RSA Implementation"
- 14h20 - 14h50 : Annelie Heuser : "Profiled side-channel analysis revisited"
- 14h50 - 15h20 : Maria Mushtaq: "Machine Learning for Security: The Case of Side-channel Attack Detection at Run-time"

- 15h20 - 15h50 : Rémi BERNHARD: "Quantization and Adversarial Machine Learning"

Participants

Cette journée a réuni 30 participants. La répartition des participants entre doctorants, chercheurs et enseignants-chercheurs du CNRS et des Universités, et membres d'organisations étatiques est la suivante :

- 8 enseignants-chercheurs
- 5 chercheurs
- 12 Doctorants
- 2 membres d'entités étatiques
- 2 membres d'un industrie

Les laboratoires et institutions académique représentés étaient les suivants : LIRMM, Laboratoire Hubert Curien, ESME, IRISA, LAMH, ETIS, LIP6, TIMA, Lab-STICC, XLIM, LCIS, IETR, VERIMAG, École central de Lyon et l'École des Mines de Saint-Etienne.

L'industriel représenté était le suivant : CEA.

Les entités étatiques représentées étaient les suivantes : ANSSI, Ministère de l'Intérieur.