RELIABILITY

TEST SECURITY

AI-TREATS

AI – TREATS

1st Workshop on

AI Hardware: Test, Reliability, and Security

(Virtual Event)

May 28, 2021

https://ai-treats-workshop.aalto.fi/

General Chairs

Haralampos-G. Stratigopoulos (FR)
Ioana Vatajelu (FR)

Program Chair

Fei Su (US)
Martin Andraud (FI)

Program Committee

TBA

Call for Contributions

Recent advances in Artificial Intelligence (AI), in particular deep learning, have led to numerous applications, including computer vision, speech recognition, natural language processing, robotics, etc. Autonomous vehicles are also afoot and AI will be the core enabling technology. In parallel, there is intense activity in designing dedicated hardware for AI. On one hand, AI hardware accelerators are demanded to support the tremendous processing power, unprecedented speed, and memory costs that deep neural networks require so as to realize their full potential. On the other hand, there is a large incentive for moving the AI algorithms execution from the cloud into the edge devices, i.e. Internet-of-Things (IoT) devices, in particular for meeting data confidentiality and network bandwidth requirements and eliminating the communication latency. Edge devices are expected to include local AI processing, yet this is challenging as an edge device is a resource-constrained environment. AI hardware design efforts rapidly evolve exploring various architectures (e.g., machine learning-based, spiking), design flavors (e.g., digital, mixed analog-digital), and emerging technologies (e.g., memristive devices arranged into crossbars to implement efficiently the multiply-add matrix operations in neural networks). The aim of this Workshop is to focus particularly on the following emerging problems pertaining to AI hardware:

- **Testing**: fault modelling, fault simulation, test generation, post-manufacturing testing, design-for-test, built-in self-test, on-line testing, fault diagnosis.
- **Reliability**: reliability analysis, design-for-reliability, fault-tolerance, self-repair, functional safety.
- **Hardware security and trust**: IP/IC piracy, hardware Trojans, side-channel attacks, fault injection attacks.

Perspective speakers are invited to submit an extended abstract of up to 2 pages or a complete 6-page paper using the submission system: **https://easychair.org/cfp/ai-treats-2021**. An informal digest of abstracts and papers will be distributed to the attendees. We seek talks on novel scientific works or preliminary results, as well as perspective talks.

.

The Workshop will take place in conjunction with the 26th IEEE European Test Symposium.

TS 21
26th IEEE European Test Symposium

Key dates:

Submission of abstracts and papers: **April 23rd, 2021**
Notification of acceptance: **April 30th, 2021**

Further Information:

Haralampos-G. Stratigopoulos – General Chair
Sorbonne Université, CNRS, LIP6
Paris, France
E-Mail: haralampos.stratigopoulos@lip6.fr

Ioana Vatajelu – General Chair
Université Grenoble Alpes, CNRS, TIMA
Grenoble, France
E-mail: ioana.vatajelu@univ-grenoble-alpes.fr

Fei Su – Program Chair
Intel
Ann Arbor, MI, USA
Email: fei.su@intel.com

Martin Andraud – Program Chair
Aalto University
Espoo, Finland
E-mail: martin.andraud@aalto.fi