4th IEEE Workshop On AI Hardware: Test, Reliability And Security (AI-TREATS)

The Hague, Netherlands, May 23-24, 2024

Program

Thursday, May 23, 2024	
16:30 – 16:35	**Opening Session** Annachiara Ruospo (Politecnico di Torino, Italy) Haralampos Stratigopoulos (Sorbonne Université, CNRS, LIP6, France)
16:35 – 17:30	**Keynote** **How does one bit-flip corrupt an entire deep neural network, and what to do about it** Yanjing Li (University of Chicago, USA)
17:30 – 18:30	**Panel** **Networks of Excellence on Edge AI in Europe** Moderator: Ihsen Alouani (Queen's University Belfast, UK) Panelists: ● Alain Pagani (German Research Center for Artificial Intelligence, Germany) – dAIEDGE project ● Matteo Sonza Reorda (Politecnico di Torino, Italy) – FAIR project ● Ovidiu Vermesan, (SINTEF, Norway) – EdgeAI project
18:30 – 19:30	**Welcome Reception**
Friday, May 24, 2024	
8:30 – 10:10	**Session 1** **High-Level Synthesis Effects on ANN Hardware Accelerator Reliability: Balancing Performance and Failure Rates (Invited)** Angeliki Kritikakou, Marcello Traiola, Fernando Fernandes Dos Santos (University of Rennes, INRIA, IRISA, France) **Exploring Hybrid Techniques for the Reliability Evaluation of TCUs** Robert Limas Sierra, Juan Guerrero, Josie Esteban Rodriguez Condia and Matteo Sonza Reorda (Politecnico di Torino, Italy)

	Functional Fault Characterization and Propagation on Systolic Arrays Salvatore Pappalardo (École Centrale de Lyon, INL, France), Alberto Bosio (École Centrale de Lyon, INL, France) and Bastien Deveautour (CPE Lyon, France) **Vulnerability Analysis of Early-Exit DNNs using hardware-aware software-level fault models** Georgios Konstantinidis, Maria Michael and Theocharis Theocharides (University of Cyprus/KIOS Research and Innovation Centre of Excellence, Cyprus) **Cost-Effective Fault Tolerance for CNNs Using Parameter Vulnerability Based Hardening and Pruning** Mohmmad Hasan Ahmadilivani (Tallinn University of Technology, Estonia), Seyedhamidreza Mousavi (Mälardalen University, Sweden), Jaan Raik (Tallinn University of Technology, Estonia), Masoud Daneshtalab (Mälardalen University, Sweden) and Maksim Jenihhin (Tallinn University of Technology, Estonia)
10:10 – 11:10	**Session 2** **CLASSES: An Open-Source Cross-Layer Error Simulation for CNNs Against Soft Errors (Invited)** Antonio Rosario Miele (Politecnico di Milano, Italy) **A Fault Injection Framework for Spiking Neural Networks** Theofilos Spyrou (TU Delft, The Netherlands) and Haralampos-G. Stratigopoulos (Sorbonne Université, CNRS, LIP6, France) **SpikingJET: Enhancing Fault Injection for Fully and Convolutional Spiking Neural Networks** Anil Bayram Gogebakan, Enrico Magliano, Alessio Carpegna, Annachiara Ruospo, Alessandro Savino and Stefano Di Carlo (Politecnico di Torino, Italy)
11:10 – 11:30	**Coffee Break**
11:30 – 12:30	**Session 3** **AI Accelerator Testing Gaps (Invited)** Moritz Fieback (TU Delft, The Netherlands)

	Test Vector Compression for the Functional Testing of AI Accelerators (Invited) Soyed Tuhin Ahmed (Chair of Dependable Nano Computing (CDNC) at KIT - Karlsruhe Institute of Technology, Karlsruhe, Germany) **Advanced Testing Techniques for AI Chips** Lee Harrison (Siemens, UK)
12:30 – 14:00	**Lunch**
14:00 – 14:40	**Session 4** **The Green Shield: Sustainable Hardware for Secure AI (Invited)** Ihsen Alouani (Queen's University Belfast, UK) **Security issues of Ultra-Low-Power Open-Source Hardware running tinyML applications** Antonio Porsia, Annachiara Ruospo and Ernesto Sanchez (Politecnico di Torino, Italy)
14:40 - 15:20	**Session 5** **Temperature-compensation of resistive in-memory-computing chips: a system perspective** Dipesh Monga (Aalto University, Finland), Gaurav Singh (Aalto University, Finland), Omar Nael Numan (Aalto University, Finland), Kari Halonen (Aalto University, Finland) and Martin Andraud (UCLouvain, Belgium) **Fully Reconfigurable AI Processing System** Rizwan Tariq Syed, Marko Andjelkovic, Markus Ulbricht and Milos Krstic (IHP, Leibniz-Institut für innovative Mikroelektronik, Germany)
15:20 – 15:30	**Closing Session** Annachiara Ruospo (Politecnico di Torino, Italy) Haralampos Stratigopoulos (Sorbonne Université, CNRS, LIP6, France)