TRUDEVICE Workshop 2014

Test and Fault Tolerance for Secure Devices

May 29th-30th, **H**einz **N**ixdorf Museums **F**orum
Paderborn (Germany)

Preliminary Program

Thursday - May 29

16:00-16:15 Welcome address

16:15-17:00 Keynote

Do you trust your chip?
Ozgur Sinanoglu (NY University Abu Dhabi, UAE)

This keynote will address trust issues and their connection with test and reliability. It will focus on the distributed design and manufacturing flow and the security vulnerabilities it creates. Counterfeiting, trojans, reverse engineering, IP piracy, and overproduction are the addressed threats. Finally, Dr Ozgur Sinanoglu, will emphasize the need to expand efforts on Design-for-Trust, an emerging IC design methodology.

17:00-17:15 Coffee Break

17:15-18:15 Hardware Trojans

17:15 Detecting Possible Locations for Hardware Trojans by Identifying Untestable Faults
Cristiana Bolchini, Luca Cassano

17:45 Stealth Assessment of Hardware Trojans in a simple Processor
I. Nikopoulos, A. Milidonis, I. Voyiatzis, C. Sgouropoulou, C. Efstathiou

Friday - May 30

9:00-10:30 Attacks

9:00 Power Supply Glitches Accuracy Analysis
Loïc Zussa, Jean-Max Dutertre, Jessy Clediere, Bruno Robisson

9:30 Simulating Laser Effects on ICs, from Physical Level to Gate Level: a Comprehensive Approach
F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre, G. Hubert

10:00 FPGA Emulation of Laser Attacks Against Secure Deep Submicron Integrated Circuits
A. Papadimitriou, D. Hély, V. Beroulle, P. Maistri, R. Leveugle

10:30-10:50 Coffee Break

10:50-12:20 Countermeasures

10:50 A Low Area Probing Detector for Security ICs
Michael Weiner, Salvador Manich, Georg Sigl

11:20 Fault Attacks on Two Software Countermeasures
Nicolas Moro, Karine Heydemann, Amine Dehbaoui, Bruno Robisson, Emmanuelle Encrenaz

11:50 Error Recovery Mechanism Using Dynamic Partial Reconfiguration
Anton Biasizzo, Franc Novak

12:20 Lunch