FDTC 2016: Final Program (PDF)

08:45 – 09:05 Registration and Early morning break

09:05 – 09:15 Opening remarks

Keynote Talk I

Chair: Luca Breveglieri

09:15 – 09:55 Attacks on encrypted memory and constructions for memory protection
Shay Gueron

Session 1 – Differential Fault Analysis

Chair: Debdeep Mukhopadhyay

09:55 – 10:20 Differential fault analysis of SHA3-224 and SHA3-256
Pei Luo, Yunsi Fei, Liwei Zhang and A. Adam Ding

10:20 – 10:45 Improved fault analysis on SIMON block cipher family
Hua Chen, Jingyi Feng, Vincent Rijmen, Yunwen Liu, Limin Fan and Wei Li

10:45 – 11:10 Morning break

Session 2 – Fault Injection-based Attacks

Chair: Wieland Fischer

11:10 – 11:35 Controlling PC on ARM using fault injection
Niek Timmers, Albert Spruyt and Marc Witteman

11:35 – 12:00 Attack on a DFA protected AES by simultaneous laser fault injections
Bodo Selmke, Johann Heyszl and Georg Sigl

12:00 – 12:25 Software fault resistance is futile: effective single-glitch attacks
Bilgiday Yuce, Nahid Farhady, Harika Santapuri, Chinmay Deshpande, Conor Patrick and Patrick Schaumont

12:25 – 13:40 Lunch

Keynote Talk II

Chair: Elke De Mulder

13:40 – 14:20 Continuous-time computational aspects of cyber-physical security
Sam Green, Ihsan Çiçek and Çetin Kaya Koç

Session 3 – Fault Sensitivity and Fault Detection

Chair: Sylvain Guilley

14:20 – 14:45 Lattice-based signature schemes and their sensitivity to fault attacks
Nina Bindel, Johannes Buchmann and Juliane Krämer

14:45 – 15:10 An embedded digital sensor against EM and BB fault injection
David El-Baze, Jean-Baptiste Rigaud and Philippe Maurine

15:10 – 15:35 Afternoon break

Session 4 – Countermeasures against Fault Attacks

Chair: Michael Hutter

15:35 – 16:00 Fault tolerant implementations of delay-based physically unclonable functions on FPGA
Durga Prasad Sahoo, Sikhar Patranabis, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty

16:00 – 16:25 Ring oscillator under laser: potential of PLL based countermeasure against laser fault injection
Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura and Makoto Nagata

16:25 – 16:50 More efficient private circuits II through threshold implementations
Thomas De Cnudde and Svetla Nikova

16:50 – 17:00 Closing remarks and Farewell