FDTC 2018: Final Program (PDF)

08:45 – 09:05 Registration

09:05 – 09:15 Opening remarks

Session 1 – Laser Fault Attacks

Chair: Laurent Sauvage (Telecom ParisTech)

9.15 – 9:45 Laser fault injection at the CMOS 28 nm technology node: an analysis of the fault model
Jean-Max Dutertre, Vincent Beroulle, Stephan De Castro, Louis-Bathelemy Faber, Marie-Lise Flottes, Philippe Gendrier, David Hely, Régis Leveugle, Paolo Maistri, Giorgio Di Natale, Athanasios Papadimitriou and Bruno Rouzeyre

9:45 – 10:15 Latch-up-locked? – An empirical study on laser fault injection into ARM Cortex-M processors
Bodo Selmke, Kilian Zinnecker, Philipp Koppermann, Katja Miller, Johann Heyszl and Georg Sigl

10:15 – 10:45 Morning break

Session 2 – Fault Attacks and Countermeasures

Chair: Begül Bilgin (Rambus)

10:45 – 11:15 Breaking redundancy-based countermeasures with random faults and power side channel
Sayandeep Saha, Shivam Bhasin, Dirmanto Jap, Jakub Breier, Debdeep Mukhopadhyay and Pallab Dasgupta

11:15 – 11:45 Darth's saber: a key exfiltration attack for symmetric ciphers using laser light
Guido Bertoni, Vittorio Zaccaria, Maria Chiara Molteni and Filippo Melzani

11:45 – 12:15 Glitch-resistant masking schemes as countermeasure against fault sensitivity analysis
Victor Arribas, Thomas De Cnudde and Danilo Sijacic

12:15 – 13:15 Lunch

Session 3 – Electromagnetic Fault Attacks

Chair: Elif Kavun (Infineon)

13:15 – 13:45 Genetic algorithm-based electromagnetic fault injection
Antun Maldini, Niels Samwel, Stjepan Picek and Lejla Batina

13:45 – 14:15 The impact of pulsed electromagnetic fault injection on true random number generators
Maxime Madau, Michel Agoyan, Josep Balash, Milos Grujic, Patrick Haddad, Philippe Maurine, Vladimir Rozic, Dave Singelee, Ingrid Verbauwhede and Bohan Yang

	Keynote Talk *Chair: Joan Daemen (Radboud Univ.)*
14:15 – 15:05	The SP800-90B approach to entropy sources *John Kelsey*
15:05 – 15:35	Afternoon break
	Panel *Moderator: Marc Witteman (Riscure)*
15:35 – 16:50	Random generator testing and evaluation *John Kelsey, Sylvain Guilley, Assia Tria, Werner Schindler*
16:50 – 17:00	Closing remarks and Farewell