FDTC 2015: Final Program

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

09:05 – 09:15 Opening remarks

Keynote Talk I

Chair: Sylvain Guilley

09:15 – 09:55 Fault Attacks at the System Level – The Challenge of Securing Application Software
Stefan Mangard

Session 1 – Fault Injection: Models and Techniques

Chair: Philippe Loubet-Moundi

09:55 – 10:20 EM Injection: Fault Model and Locality
Sebastien Ordas, Ludovic Guillaume-Sage and Philippe Maurine

10:20 – 10:45 On the Complexity Reduction of Laser Fault Injection Campaigns using OBIC Measurements
Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schaepers, Nils Gerhardt, Martin Hofmann and Christof Paar

10:45 – 11:10 Morning break

Session 2 – DFA: Models and Techniques

Chair: Guido Bertoni

11:10 – 11:35 Improved Differential Fault Attack on the Block Cipher SPECK
Yuming Huo, Fan Zhang, Xiutao Feng and Li-Ping Wang

11:35 – 12:00 J-DFA: A Novel Approach for Robust Differential Fault Analysis
Luca Magri, Silvia Mella, Filippo Melzani, Pasqualina Fragneto and Beatrice Rossi

12:00 – 12:25 Lost in Translation: Fault Analysis of Infective Security Proofs
Alberto Battistello and Christophe Giraudy

12:25 – 13:40 Lunch

Keynote Talk II

Chair: Francesco Regazzoni

13:40 – 14:20 The Need for Intrinsic Hardware Security below 65 nm
Mathias Wagner

Session 3 – Fault Injection Attacks to Cipher Families

Chair: Naofumi Homma

14:20 – 14:45 To Exploit Fault Injection on non-Injective Sboxes
Guillaume Bethouart and Nicolas Debande

14:45 – 15:10 An Efficient One-Bit Model for Differential Fault Analysis on Simon Family
Juan Grados, Fabio Borges, Renato Portugal and Pedro Lara

15:10 – 15:35 Afternoon break

Session 4 – Fault Attacks to Cryptographic Devices
Chair: Victor Lomné

15:35 – 16:00 Singular Curve Point Decompression Attack
Johannes Blömer and Peter Günther

16:00 – 16:25 Laser Fault Attack on Physically Unclonable Functions
Shahin Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert and Christian Boit

16:25 – 16:50 Improving Fault Attacks on Embedded Software using RISC Pipeline Characterization
Bilgiday Yuce, Nahid Farhady Ghalaty and Patrick Schaumont

16:50 – 17:00 Closing remarks and Farewell