FDTC 2022: Final Program (PDF)

FDTC 2022 is a Virtual Conference (Zoom Webinar)

Schedule refers to Central European Summer Time (CEST)

Start: 10:00 CEST (04:00 am New York – 05:00 pm Tokyo)

10:00 – 10:10 Welcome and Opening remarks

Keynote I

Chair: Shivam Bhasin

10:10 – 10:50 Statistical Ineffective Fault Attacks (SIFA)
Florian Mendel

10:50 – 11:00 Break

Session 1 – Laser Fault Attacks

Chair: Luca Breveglieri

11:00 – 11:15 Embedded-EEPROM descrambling via laser-based techniques – A case study on AVR MCU
Samuel Chef, Chung Tah Chua, Jing Yun Tay, Jason Jun Wei Cheah and Chee Lip Gan

11:15 – 11:30 Triple Exploit Chain with Laser Fault Injection on a Secure Element
Olivier Hériveaux

11:30 – 11:45 The More You Know: Improving Laser Fault Injection with Prior Knowledge
Marina Krček, Thomas Ordas, Daniele Fronte and Stjepan Picek

11:45 – 12:00 Break

Session 2 – Fault Attacks to Public Key Cryptosystems

Chair: Luca Breveglieri

12:00 – 12:15 FA-LLLing for RSA: Lattice-based Fault Attacks against RSA Encryption and Signature
Guillaume Barbu

12:15 – 12:30 Generalising Fault Attacks to Genus Two Isogeny Cryptosystems
Ariana Goh, Chu-Wee Lim and Yan Bo Ti

12:30 – 13:15 Break

Session 3 – Fault Injection: Techniques, Analysis, Effects

Chair: Luca Breveglieri

13:15 – 13:30 Body Biasing Injection: Impact of substrate types on the induced disturbances?
Geoffrey Chancel, Jean-Marc Gallière and Philippe Maurine

13:30 – 13:45 Quantifying the Speed-Up Offered by Genetic Algorithms during Fault Injection Cartographies
Idris Rais-Ali, Antoine Bouvet and Sylvain Guilley

13:45 – 14:00 Exploration of Fault Effects on Formal RISC-V Microarchitecture Models
Simon Tollec, Mihail Asavoae, Damien Couroussé, Karine Heydemann and Mathieu Jan

14:00 – 14:10 Break

Keynote II

Chair: Luca Breveglieri

14:10 – 14:50 Pre-silicon fault simulation: hard and important
Jasper van Woudenberg

14:50 – 15:00 Closing remarks and Farewell