FDTC 2023: Final Program

09:15 – 09:30 Welcome and Opening remarks

Keynote

Chair: Pascal Sasdrich

09:30 – 10:30 Fault attack friendliness of post-quantum cryptosystems
Alessandro Barenghi *and Gerardo Pelosi*

10:30 – 11:00 Break

Session 1 – Fault Attack Models and Countermeasures

Chair: Łukasz Chmielewski

11:00 – 11:30 A tale of two models: discussing the timing and sampling EM fault injection models
Jean-Luc Danger, Jean-Max Dutertre, ***Roukoz Nabhan****, Jean-Baptiste Rigaud and Laurent Sauvage*

11:30 – 12:00 Voronoi based multidimensional parameter optimization for fault injection attacks
Marius Eggert and ***Marc Stöttinger***

12:00 – 12:30 A compositional methodology to harden programs against multi-faults attacks
Etienne Boespflug*, Abderrahmane Bouguern, Mounier Laurent and Marie-Laure Potet*

12:30 – 14:00 Lunch

Session 2 – Fault Injection Analysis and Tools

Chair: Falk Schellenberg

14:00 – 14:30 Analysis of arbitrary waveform generation for voltage glitches
Vincent Immler *and Stanislav Lyakhov*

14:30 – 15:00 A better practice of body biasing injection
Geoffrey Chancel*, Jean-Marc Gallière and Philippe Maurine*

15:00 – 15:30 PicoEMP: a low-cost EMFI platform compared to BBI and voltage fault injection using TDC & external VCC measurements
Colin O'Flynn

15:30 – 16:00 Break

Session 3 – Fault Attacks on SW and HW Devices

Chair: Alessandro Barenghi

16:00 – 16:30 Fault attacks on a cloud-assisted ECDSA white-box based on the residue number system
Christophe Giraud and ***Agathe Houzelot***

16:30 – 17:00 Forging DILITHIUM and FALCON signatures by single fault injection
Sven Bauer *and Fabrizio De Santis*

17:00 – 17:30	DeepCover DS28C36: a hardware vulnerability identification and exploitation using T-test and double laser fault injection ***Karim Abdellatif*** *and Olivier Hériveaux*
17:30 – 17:40	Closing remarks and Farewell