FDTC 2024: Final Program

09:30 – 09:40 Welcome and Opening remarks

Keynote I

Chair: Francesco Regazzoni

09:40 – 10:30 Persistent Fault Analysis: The Persistent Threat
Shivam Bhasin

10:30 – 11:00 Coffee Break

Session 1 – FAULT ATTACKS ON SW AND HW DEVICES

Chair: Victor Lomné

11:00 – 11:30 A single-trace fault injection attack on hedged module lattice digital signature algorithm (ML-DSA)
Sönke Jendral*, John Preuß Mattsson and Elena Dubrova*

11:30 – 12:00 Fault injection attacks exploiting high voltage pulsing over Si-substrate backside of IC chips
Yusuke Hayashi*, Rikuu Hasegawa, Takuya Wadatsumi, Kazuki Monta, Takuji Miki and Makoto Nagata*

12:00 – 12:30 Improving CPU fault injection simulations: insights from RTL to instruction-level models
Jasper van Woudenberg*, Rajesh Velegalati, Cees-Bart Breunesse and Dennis Vermoen*

12:30 – 13:30 Lunch

Keynote II

Chair: Makoto Nagata

13:30 – 14:20 Fault Tolerance of Encrypted Memory: Crash Consistency Problem and Secure Recovery
Rei Ueno

Session 2 – FAULT ATTACK MODELS AND COUNTERMEASURE (short papers)

Chair: Wieland Fischer

14:20 – 14:40 Switch-glitch - location of fault injection sweet spots by electromagnetic emanation
Matthias Probst*, Michael Gruber, Manuel Brosch, Tim Music and Georg Sigl*

45:40 – 15:00 MAYo or MAY-not: exploring implementation security of the post-quantum signature scheme MAYO against physical attacks
Thomas Aulbach, Soundes Marzougui, ***Vincent Quentin Ulitzsch*** *and Jean-Pierre Seifert*

15:00 – 15:30 Coffee Break

Session 3 – Fault Injection Analysis and Tools

Chair: Rei Ueno

15:30 – 16:00 FaultyGarble: fault attack on secure multiparty neural network inference
Mohammad Hashemi, Dev Mehta, Kyle Mitard, Shahin Tajik and ***Fatemeh Ganji***

16:00 – 15:30 PoP DRAM: a new EMFI approach based on EM-induced glitches on SoC
Clément Fanjas*, Simon Pontié, Driss Aboulkassimi and Jessy Clédierè*

16:30 – 16:45 Closing remarks and Farewell