

FDTC 2026: Final Program (PDF)

all times are in Turkey Time (TRT – UTC+3)

start: 08:00 am Rome – 02:00 am NY – 03:00 pm Tokyo

presenting authors are highlighted in red

09:00 – 09:15 Welcome and Opening remarks

Session 1 – Fault Injection Platforms & Practical Attacks

Chair: Victor Lomné

- 09:15 – 09:40 BitCrusher: Affordable, Open Source, Electromagnetic Fault Injection Platform
George Crane and Dean Sullivan
- 09:40 – 10:05 Repurposing Inexpensive Laser Welder for Laser Fault Injection
Kensho Murata, Yujin Mori, Soramichi Akiyama and Takeshi Sugawara
- 10:05 – 10:30 Glitching Firmware Readout Protection in an EV Charger and Instrument Cluster: Case Studies on GD32 and RH850 MCUs
Niclas Kühnapfel, Mahsa Kholghi, Kai Jansen, Christian Zenger and Jean-Pierre Seifert
- 10:30 – 11:00 Coffee Break

Session 2 – Fault Attacks on Post-Quantum Cryptography

Chair: Gerardo Pelosi

- 11:00 – 11:25 Oil, Vinegar, and Sparks: Key Recovery from UOV via Single Electromagnetic Fault Injection
Fabio Campos, **Daniel Hahn**, Daniel Könnecke and Marc Stöttinger
- 11:25 – 11:50 Practical End-to-end Fault Attacks on PERK
Tanguy Stekke, **Durba Chatterjee** and Lejla Batina
- 11:50 – 12:05 Revisiting Correction Attack on CROSS: Improved Attack Method through Analyzing Power Traces (short presentation)
Xiao Huang, Chao Sun and Mehdi Tibouchi
- 12:05 – 12:20 Learning with Errors and Omissions: the Case for Fujisaki-Okamoto Checks on ML-KEM Decapsulation Keys (short presentation)
Daniel Shiu
- 12:20 – 13:30 Lunch

Session 3 – Fault Attacks on Crypto Primitives & Hardware

Chair: Alessandro Barenghi

- 13:30 – 13:55 Fault Attack on PLL-TRNG: Randomness Degradation through Clock Glitch-Induced PLL Perturbation
Hikaru Nishiyama, Daisuke Fujimoto, Shinichi Kawamura and Yuichi Hayashi
- 13:55 – 14:20 Breaking the One-Way Property of a SHA-3 Implementation via Fault Injection
Mona Sobhani, Sönke Jendral, Mats Näslund and Elena Dubrova
- 14:20 – 14:45 Bridging Laser Fault Injection Experiments and Pre-Silicon Analysis on AES Hardware
Giorgio Fardo, Damien Courousse, Mathieu Jan, Laurent Maingault and Loïc Mangin
- 14:45 – 15:00 Do MCUs Dream of Electric Earth? Revisiting Voltage Fault Injection Through Ground Manipulation (short presentation)
Xhani Marvin Saß, **Ran Zhang** and Jean-Pierre Seifert
- 15:00 – 15:30 Coffee Break

Session 4 – Countermeasures and Formal Analysis

Chair: Thorben Moos

- 15:30 – 15:55 Study of Rust's Attack Surface Against Multiple Fault Injection
Etienne Boespflug, Tommy Prats, Timothé Baleras and Laurent Mounier
- 15:55 – 16:20 Reverse to Reveal: Reversibility as a Fault Defense
Xhani Marvin Saß, **Meng Yuan** and Jean-Pierre Seifert
- 16:20 – 16:35 Structure-Aware Software Resilience for Number Theoretic Transforms (short presentation)
Ro Cammarota, Brittany Liu, Caroline Wang, Nahid Farhady, **Jayanta Chowdhury**, Elif Bilge Kavun and Igor Nunes
- 16:35 – 16:50 Layout-Aware Incremental Formal Fault Injection (short presentation)
Félix Ridoux, Florian Talon, Souheib Baarir, Jean-Marc Daveau and Philippe Roche
- 16:50 – 17:00 Closing remarks and Farewell