

**Fault Diagnosis and
Tolerance in Cryptography**

Fault Diagnosis and Tolerance in Cryptography 2026

Robert Buhren¹

Shahin Tajik²

¹AMD General & Technische Universität Berlin

²Worcester Institute of Technology

11 October, 2026 – Antalya, Turkey

Chairs

Program:

Robert Buhren
Shahin Tajik

AMD General & Tech. Univ. Berlin
Worcester Institute of Technology

General:

Michael Tunstall

Google

Publication:

Luca Breveglieri

Politecnico di Milano

Finance:

Israel Koren

University of Massachusetts

Sponsorship:

Fabrizio De Santis

Siemens

Steering Committee:

Luca Breveglieri

Politecnico di Milano

Israel Koren

University of Massachusetts

David Naccache

ENS de Paris

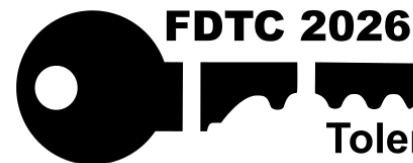
Jean-Pierre Seifert

TU Berlin

Sponsors – Thank You!



Program Committee



Fault Diagnosis and
Tolerance in Cryptography

Aydin Aysu, *NC State University, USA*

Sven Bauer, *Siemens AG, Germany*

Shivam Bhasin, *NTU, Singapore*

Sarani Bhattacharya, *IIT Kharagpur, India*

Lilian Bossuet, *University of Lyon, France*

Guillaume Bouffard, *ANSSI, France*

Jakub Breier, *Silicon Austria Labs, Austria*

Robert Buhren (co-chair), AMD General & Technische Universität Berlin, Germany

Durba Chatterjee, *Radboud University, The Netherlands*

Wieland Fischer, *Infineon Technologies, Germany*

Domenic Forte, *University of Florida, USA*

Fatemeh Ganji, *Worcester Polytechnic Institute, USA*

Christophe Giraud, *IDEMIA, France*

Yuichi Hayashi, *Nara Institute of Science and Technology, Japan*

Daniel Holcomb, *University of Massachusetts at Amherst, USA*

Thilo Krachenfels, *AMD, Germany*

Juliane Krämer, *University of Regensburg, Germany*

Thorben Moos, *Université Catholique de Louvain, Belgium*

David Naccache, *Ecole Normale Supérieure, France*

Hamed Okhravi, *MIT Lincoln Laboratory, USA*

Pascal Sasdrich, *Ruhr University Bochum, Germany*

Okan Seker, *NXP Semiconductors, The Netherlands*

Takeshi Sugawara, *University of Electro-Communications, Japan*

Dean Sullivan, *University of New Hampshire, USA*

Shahin Tajik (co-chair), Worcester Polytechnic Institute, USA

Rei Ueno, *Kyoto University, Japan*

Vincent Ulitzsch, *Massachusetts Institute of Technology, USA*

Victor van-der-Veen, *Vrije Universiteit Amsterdam, The Netherlands*

Qifan Wang, *Durham University, United Kingdom*

Submitted Papers

- 22 papers submitted
- reviewed by PC members and additional reviewers
- all papers received three reviews

Accepted Papers

- 10 regular papers (around 45%)
- 5 short papers (around 23%)
- 15 total papers (around 68%)

Proceedings – to come

the proceedings will be published by [CPS](#) (on IEEExplore)

Program Schedule

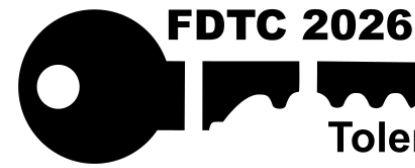


Session 1 – Fault Injection Platforms & Practical Attacks

Chair: Victor Lomné

- | | |
|---------------|--|
| 09:15 – 09:40 | BitCrusher: Affordable, Open Source, Electromagnetic Fault Injection Platform
<i>George Crane</i> and Dean Sullivan |
| 09:40 – 10:05 | Repurposing Inexpensive Laser Welder for Laser Fault Injection
<i>Kensho Murata</i> , 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
<i>Niclas Kühnapfel</i> , Mahsa Kholghi, Kai Jansen, Christian Zenger and Jean-Pierre Seifert |
| 10:30 – 11:00 | Coffee Break |

Program Schedule



FDTC 2026

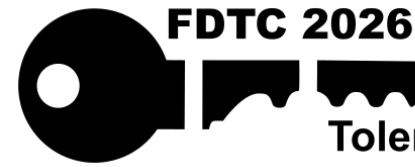
Fault Diagnosis and
Tolerance in Cryptography

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
<i>Fabio Campos, Daniel Hahn, Daniel Könnecke and Marc Stöttinger</i> |
| 11:25 – 11:50 | Practical End-to-end Fault Attacks on PERK
<i>Tanguy Stekke, Durba Chatterjee and Lejla Batina</i> |
| 11:50 – 12:05 | Revisiting Correction Attack on CROSS: Improved Attack Method through Analyzing Power Traces (short presentation)
<i>Xiao Huang, Chao Sun and Mehdi Tibouchi</i> |
| 12:05 – 12:20 | Learning with Errors and Omissions: the Case for Fujisaki-Okamoto Checks on ML-KEM Decapsulation Keys (short presentation)
<i>Daniel Shiu</i> |
| 12:20 – 13:30 | Lunch |

Program Schedule



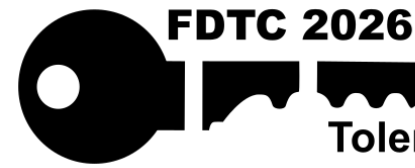
Fault Diagnosis and
Tolerance in Cryptography

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 |

Program Schedule



Fault Diagnosis and
Tolerance in Cryptography

Session 4 – Countermeasures and Formal Analysis

Chair: Thorben Moos

- | | |
|---------------|---|
| 15:30 – 15:55 | Study of Rust's Attack Surface Against Multiple Fault Injection
<i>Etienne Boespflug</i> , Tommy Prats, Timoth   Baleras and Laurent Mounier |
| 15:55 – 16:20 | Reverse to Reveal: Reversibility as a Fault Defense
Xhani Marvin Sa  , <i>Meng Yuan</i> 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, <i>Jayanta Chowdhury</i> , Elif Bilge Kavun and Igor Nunes |
| 16:35 – 16:50 | Layout-Aware Incremental Formal Fault Injection (short presentation)
<i>F  lix Ridoux</i> , Florian Talon, Souheib Baarir, Jean-Marc Daveau and Philippe Roche |
| 16:50 – 17:00 | Closing remarks and Farewell |

Congratulations to all the Authors
Wishing you a wonderful FDTC 2026!

[FDTC workshop series \(since 2004\)](https://fdtc-workshop.eu)

<https://fdtc-workshop.eu>