



Fault Diagnosis and Tolerance in Cryptography 2025

Alessandro Barenghi¹

Juliane Krämer²

¹Politecnico di Milano, Italy

²Universität Regensburg, Germany

14 September, 2025 – Kuala Lumpur, Malaysia

Chairs



- **Program:** **Alessandro Barenghi**
Juliane Krämer
- **General:** **Michael Tunstall**
- **Publication:** **Luca Breveglieri**
- **Finance:** **Israel Koren**
- **Sponsorship:** **Fabrizio De Santis**

Politecnico di Milano, Italy
Universität Regensburg, Germany

Google
Politecnico di Milano
University of Massachusetts
Siemens

Steering Committee:

- **Luca Breveglieri**
- **Israel Koren**
- **David Naccache**
- **Jean-Pierre Seifert**

Politecnico di Milano
University of Massachusetts
ENS de Paris
TU Berlin

Sponsors – Thank You!



Program Committee



Elham	Amini	TU Berlin, DE
Diego	Aranha	Aarhus University, DK
Aydin	Aysu	NC State University, US
Melissa	Azouaoui	NXP, DE
Josep	Balasz	Katholieke Universiteit Leuven, BE
Sven	Bauer	Siemens AG, DE
Davide	Bellizia	Telsy, IT
Sarani	Bhattacharya	IIT Kharagpur, IN
Shivam	Bhasin	NTU, SG
Guillaume	Bouffard	ANSSI, FR
Jakub	Breier	Silicon Austria Labs, AT
Ileana	Buhan	Radboud University, NL
Fabrizio	De Santis	Siemens, DE
Elena	Dubrova	Royal Inst. of Technology (KTH), SE
Jean-Max	Dutertre	Ecole des Mines de Saint-Etienne, FR
Wieland	Fischer	Infineon Technologies, DE
Fatemeh	Ganji	Worcester Polytechnic Institute, US
Christophe	Giraud	IDEMIA, FR

Osnat	Keren	Bar-Ilan University, IL
Victor	Lomné	NinjaLab, FR
Soundes	Marzougui	STM, BE
Mehran	Mozaffari Kermani	University of South Florida, US
David	Oswald	The University of Birmingham, UK
Gerardo	Pelosi	Politecnico di Milano, IT
Stjepan	Picek	Radboud University, NL
Francesco	Regazzoni	Univ. Amsterdam & UNISI, NL & CH
Chester	Rebeiro	IIT Madras, IN
Sayandeep	Saha	IIT Bombay, IN
Pascal	Sasdrich	Ruhr University Bochum, DE
Georg	Sigl	Tech. Universitaet Muenchen, DE
Sergei	Skorobogatov	University of Cambridge, UK
Marc	Stöttinger	RheinMain Univ. Applied Sci., DE
Takeshi	Sugawara	Univ. of Electro-Comm., JP
Junko	Takahashi	NTT, JP
Rei	Ueno	Kyoto University, JP
Fan	Zhang	Zhejiang University, CN

Submitted Papers

- 12 papers submitted
- reviewed by PC members and additional reviewers
- most papers received 3 reviews

Accepted Papers

- 7 regular papers (around 58%)
- 1 short paper (around 8%)

Proceedings – webpub

- paper URL: <https://conferences.computer.org/fdtcpub25>
- login: fdtcpub25 (to be closed few days after FDTC)
- password: conf25// (please include also the two slashes)

The proceedings will be published by CPS (on IEEExplore).

Invited Talks

- ***Fault Injection in System Design and Verification:
Challenges and Future Directions***

- *Tim Güneysu*
- Ruhr Universität



- ***Empowering Research on AMD CPUs: Open Access
to Advanced Fault Injection Capabilities***

- *Hans Niklas Jacob*
- Tu Berlin



Program Schedule



09:00 – 09:10 Welcome and Opening remarks

Keynote I

Chair: TBD

09:10 – 10:00 Fault injection in system design and verification: challenges and future directions
Tim Güneysu

Program Schedule



Session 1 – FAULT DETECTION AND ANALYSIS

Chair: TBD

- | | |
|---------------|--|
| 10:00 – 10:30 | AutoPulse – reproducible discovery of electromagnetic fault injection vulnerabilities
<i>Ingmar Baumgart, Jonathan Kramer, Maximilian Staab and Marek Wehmer</i> |
| 10:30 – 11:00 | Coffee Break |
| 11:00 – 11:30 | Fault detection in the control and data-path of neural networks
<i>Manuel Brosch, Augustin Ewald, Michael Gruber, Matthias Probst and Georg Sigl</i> |
| 11:30 – 12:00 | Improving fault vulnerability detection via rehosting and comparative analysis of open-source tools
Shoei Nashimoto |
| 12:00 – 12:30 | Fault analysis through body bias injection on the FLASH memory accelerator of a microcontroller
<i>Florent Bruguier, Ziling Liao and Philippe Maurine</i> |
| 12:30 – 14:10 | Lunch |

Program Schedule



Keynote II

Chair: TBD

14:10 – 15:00	Empowering research on AMD CPUs: open access to advanced fault injection capabilities <i>Hans Niklas Jacob</i>
---------------	--

Program Schedule



Session 2 – FAULT MODELS AND ATTACKS

Chair: TBD

- | | |
|---------------|--|
| 15:00 – 15:30 | From NOP to ADD and beyond: a novel fault-model comprising variable-length instruction sets
<i>Xhani Marvin Saß</i> , Thomas Martin Johannes Lehrach and Jean-Pierre Seifert |
| 15:30 – 16:00 | Coffee Break |
| 16:00 – 16:30 | Fault attacks against UOV-based signatures
<i>Sven Bauer</i> , Fabrizio De Santis and Kristjane Koleci |
| 16:30 – 17:00 | SIFA on nonce-based authenticated encryption: when does it fail?
Application to Ascon
Pierre-Louis Cayrel, Vincent Grosso and <i>Viet-Sang Nguyen</i> |
| 17:30 – 17:15 | Closing remarks and Farewell |

Congratulations to all the Authors
Wishing you a wonderful FDTC 2025!

[FDTC workshop series \(since 2004\)](#)

fdtc-workshop.eu