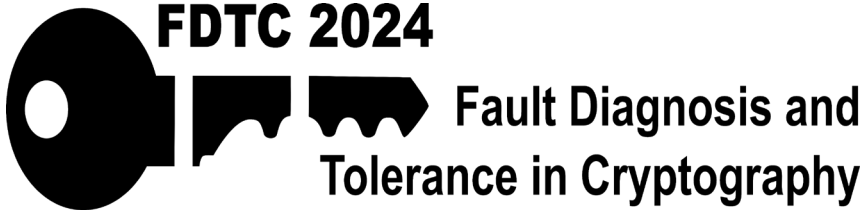


Fault Diagnoses and Tolerance in Cryptography 2024

Fabrizio De Santis[1] **Francesco Regazzoni**[2]

[1]Siemens, Germany [2]Univ. of Amsterdam & UniSI, The Netherlands & Switzerland

4 September, 2024 – Halifax, Nova Scotia, Canada

Chairs

FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

• **Program**:	**Fabrizio De Santis** **Francesco Regazzoni**	*Siemens*, Germany *Univ. of Amsterdam* & *UniSI*, The Netherlands & Switzerland
• **General**:	**Michael Tunstall**	*Google*
• **Publication**:	**Luca Breveglieri**	*Politecnico di Milano*
• **Finance**:	**Israel Koren**	*University of Massachusetts*

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!

FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

POLITECNICO
MILANO 1863

UMASS
AMHERST

Google

infineon

NewAE
Technology

riscure

SIEMENS

Program Committee

FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

Diego	Aranha	Aarhus University, DK
Aydin	Aysu	NC State University, US
Melissa	Azouaoui	NXP, DE
Josep	Balasch	Katholieke Universiteit Leuven, BE
Alessandro	Barenghi	Politecnico di Milano, IT
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
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
Juliane	Krämer	University of Regensburg, DE
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
Chester	Rebeiro	IIT Madras, IN
Sayandeep	Saha	IIT Bombay, IN
Pascal	Sasdrich	Ruhr University Bochum, DE
Georg	Sigl	Technische Universitaet Muenchen, DE
Sergei	Skorobogatov	University of Cambridge, UK
Marc	Stöttinger	RheinMain University of Applied Science, DE
Takeshi	Sugawara	The University of Electro-Communications, JP
Shahin	Tajik	Worcester Polytechnic Institute, US
Junko	Takahashi	NTT, JP
Rei	Ueno	Kyoto University, JP
Praveen	Vadnala	Riscure, NL
Fan	Zhang	Zhejiang University, CN

FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

Submitted Papers

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

Accepted Papers

- 5 regular papers (around 55%)
- 2 short papers (around 22%)

Proceedings

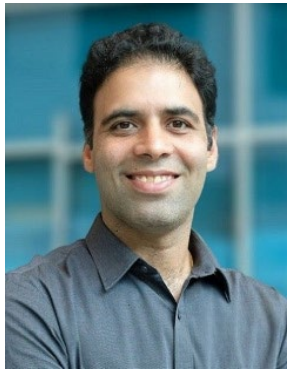
- paper URL: https://conferences.computer.org/fdtcpub24
- login: fdtcpub24 (to be closed few days after FDTC)
- password: conf24// (please include also the two slashes)

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

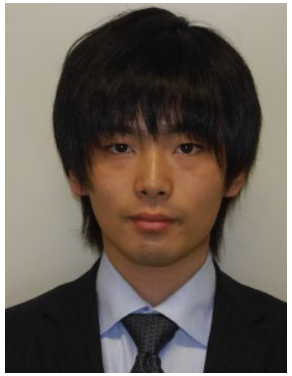
FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

Invited Talks

- ***Persistent Fault Analysis: The Persistent Threat***
  - *Shivam Bhasin*
  - Temasek Lab & Nanyang University



- ***Fault Tolerance of Encrypted Memory: Crash Consistency Problem and Secure Recovery***
  - *Rei Ueno*
  - University of Kyoto



Program Schedule

FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

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

FDTC 2024

Fault Diagnosis and Tolerance in Cryptography

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

FDTC 2024

Fault Diagnosis and Tolerance in Cryptography

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)

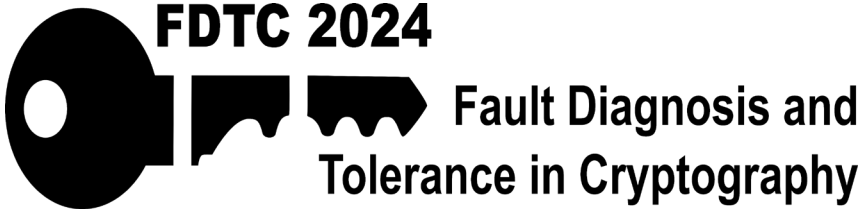
Chair: Wieland Fischer

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



Congratulations to all the Authors
Wishing you a wonderful FDTC 2024!