FDTC 2021
Fault Diagnosis and
Tolerance in Cryptography

Fault Diagnoses and Tolerance in Cryptography 2021

Debdeep Mukhopadhyay [1] **Emmanuel Prouff [2]**

[1]IIT Kharagpur & [2]ANSSI

17 September, 2021 – cyberspace

FDTC 2021 Fault Diagnosis and Tolerance in Cryptography

Chairs

• Program:	**Debdeep Mukhopadhyay**	Indian Institute of Technology Kharagpur
	Emmanuel Prouff	*ANSSI*
• General:	**Michael Tunstall**	*Rambus Cryptography Research*
• 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 & T-Labs

FDTC 2021
Fault Diagnosis and
Tolerance in Cryptography

Sponsors – Thank You!

POLITECNICO
MILANO

UNIVERSITY OF MASSACHUSETTS AMHERST 1863
UMASS
AMHERST

THALES

infineon

riscure
Visit our free online workshop
www.riscure.com/workshop-live

Rambus

TII
Technology
Innovation
Institute

NewAE
Technology

FDTC 2021

Fault Diagnosis and Tolerance in Cryptography

Program Committee

Michel Agoyan	ST Microelectronics
Josep Balasch	KU Leuven
Lejla Batina	Radboud University
Shivam Bhasin	NTU Singapore
Luca Breveglieri	Politecnico di Milano
Ileana Buhan	Riscure
Jessy Clédière	CEA LETI
Jean-Max Dutertre	ENS Mines S. Etienne
Wieland Fischer	Infineon AG
Christophe Giraud	Idemia
Jorge Guajardo	Bosch US
Sylvain Guilley	Telecom ParisTech
Olivier Hériveaux	Ledger
Johann Heyszl	Fraunhofer Institute
Osnat Keren	Bar Ilan University
Israel Koren	University of Massachusetts
Victor Lomné	Ninjalab
Philippe Loubet Moundi	Gemalto
Philippe Maurine	University of Montpellier

Joan Mazenc	Thales
Mehran Mozaffari Kermani	University of South Florida
Cristofaro Mune	Realize
Colin O’Flynn	Newae
David Oswald	University of Birmingham
Sikhar Patranabis	Visa Research
Gerardo Pelosi	Politecnico di Milano
Ilia Polian	University of Passau
Robert Primas	TU Graz
Chester Rebeiro	IIT Madras
Lionel Rivière	eShard
Falk Schellenberg	Ruhr-UniversitÂ¨at Bochum
Sergei Skorobogatov	University of Cambridge
Takeshi Sugawara	UEC Tokyo
Junko Takahashi	NTT
Shahin Tajik	University of Florida
Christian Toulemont	SERMA
Michael Tunstall	Cryptography Research
Vincent Verneuil	NXP Semiconductors
Fan Zhang	Zhejiang University

Changes to Submission Process

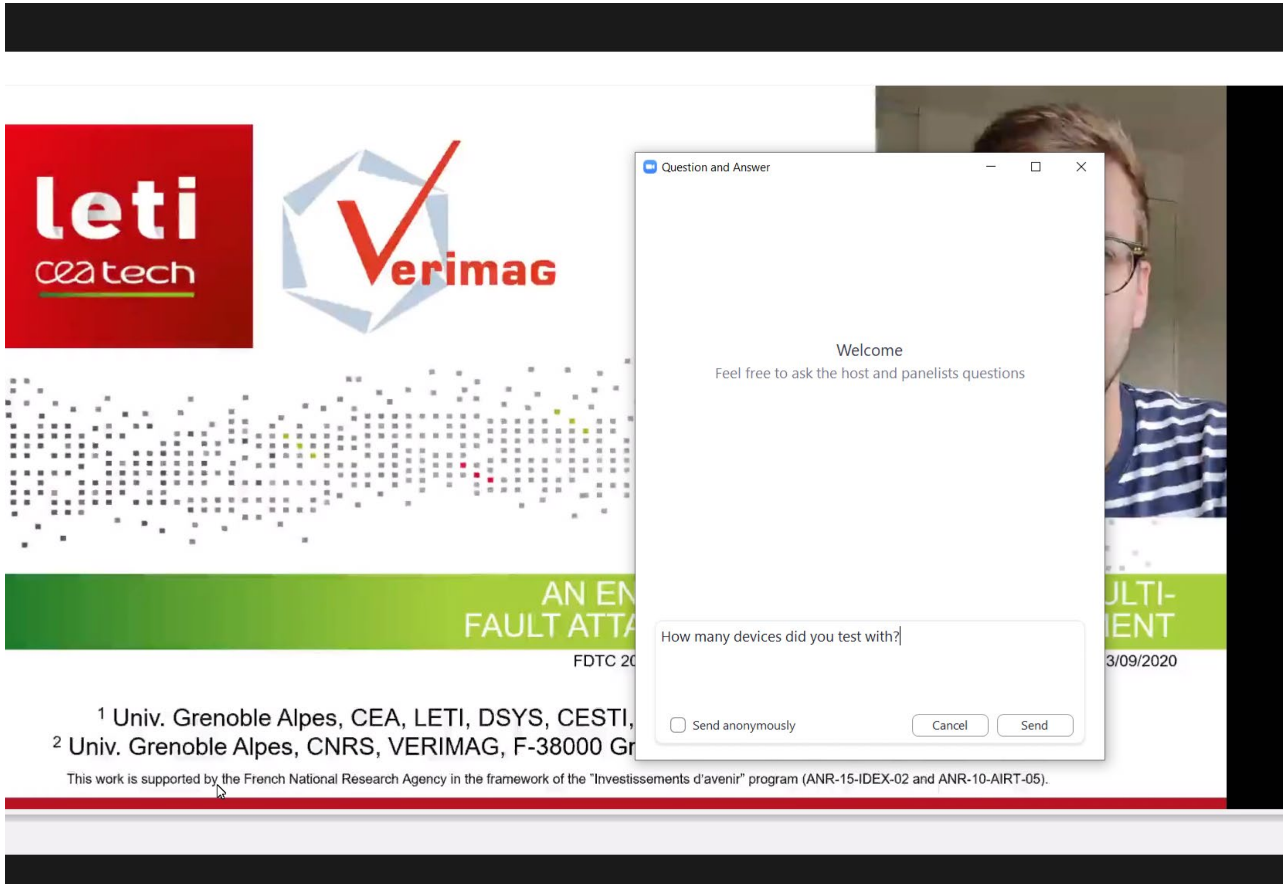
This year is the first time that we proposed to submit “Short Papers”

- the objective was to encourage submissions of works in progress or new minor results

FDTC 2021
Fault Diagnosis and
Tolerance in Cryptography

Zoom Conference Notes

- Please use the **Q&A function** to ask questions.
- Please use the **chat function** for general conference chat.



[1] Univ. Grenoble Alpes, CEA, LETI, DSYS, CESTI,
[2] Univ. Grenoble Alpes, CNRS, VERIMAG, F-38000 Gr

This work is supported by the French National Research Agency in the framework of the "Investissements d'avenir" program (ANR-15-IDEX-02 and ANR-10-AIRT-05).

Question and Answer

Welcome
Feel free to ask the host and panelists questions

How many devices did you test with?

Papers

Submitted Papers:

- 17 papers submitted
- Reviewed with PC members and additional reviewers
- Most papers received 3 reviews.

Accepted Papers:

- 7 regular papers (around 40%)
- 4 short papers (around 25%)
- Overall, Around 65% acceptance rate

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

Program Schedule – Morning 1

FDTC 2021
Fault Diagnosis and
Tolerance in Cryptography

	Start: 09:15 CEST (03:15 am New York – 04:15 pm Tokyo)
09:15 – 09:30	Opening remarks
	Keynote I *Chair: Luca Breveglieri*
09:30 – 10:20	Managing Natural Hazards and Adversarial Fault Injections in the Context of Connected Emebedded Systems *Sylvain Guilley*
10:20 – 10:50	Break

Program Schedule – Morning 2

Session 1 – Fault Analysis *Chair: Shivam Bhasin*

10:50 – 11:15	On the Importance of Initial Solutions Selection in Fault Injection *Marina Krček, Daniele Fronte and Stjepan Picek*
11:15 – 11:40	A High-Order Infective Countermeasure Framework *Guillaume Barbu, Luk Bettale, Laurent Castelnovi, Thomas Chabrier, Nicolas Debande, Christophe Giraud and Nathan Reboud*
11:40 – 12:05	ARCHIE: A QEMU-Based Framework for Architecture-Independent Evaluation of Faults *Florian Hauschild, Kathrin Garb, Lukas Auer, Bodo Selmke and Johannes Obermaier*
12:05 – 12:30	EM Fault Model Characterization on SoCs: From Different Architectures to the Same Fault Model *Thomas Trouchkine, Guillaume Bouffard and Jessy Clédière*
12:30 – 13:30	Lunch

Program Schedule – Afternoon 1

Session 2 – Short Presentations *Chair: Guillaume Bouffard*

13:30 – 13:45	Safe-Error Analysis of Post-Quantum Cryptography Algorithms *Luk Bettale, Simon Montoya and Guénaël Renault*
13:45 – 14:00	Algebraic Fault Analysis of Subterranean 2.0 *Michael Gruber, Patrick Karl and Georg Sigl*
14:00 – 14:15	Are Cold Boot Attacks still Feasible: A Case Study on Raspberry Pi with Stacked Memory *Yoo-Seung Won and Shivam Bhasin*
14:15 – 14:30	EMFI for Safety-Critical Testing of Automotive Systems *Colin O'Flynn*

Keynote II *Chair: Luca Breveglieri*

14:30 – 15:20	Fault Attacks against your Zen *Jean-Pierre Seifert*
15:20 – 15:50	Break

FDTC 2021
Fault Diagnosis and
Tolerance in Cryptography

Program Schedule – Afternoon 2

	Session 3 – Experimentation on Fault Attacks *Chair: Victor Lomné*
15:50 – 16:15	On the Scaling of EMFI Probe *Julien Toulemont, Geoffrey Chance, Jean-Marc Galliere, Frederick Mailly, Pascal Nouet and Philippe Maurine*
16:15 – 16:40	Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline *Vanthanh Khuat, Jean-Luc Danger and Jean-Max Dutertre*
16:40 – 17:05	The Forgotten Threat of Voltage Glitching: A Case Study on Nvidia Tegra X2 SoCs *Otto Bittner, Thilo Krachenfels, Andreas Galauner and Jean-Pierre Seifert*
	Panel Discussion *Moderator: Sylvain Guilley*
17:05 – 17:55	Electromagnetic Disturbance in the Industry *Arthur Beckers, Philippe Maurine, Colin O'Flynn and Stjepan Picek* New capabilities have emerged where electromagnetic (EM) benchs are used to cryptanalyze chips. The progress of this "research field" is fast, in terms of reproducibility, accuracy and number of use cases. Yet there is not enough awareness about such advances and their security threats. We discuss quantitative metrics to assess the harmfulness of EM fault injection (EMFI), so as to allow for a pre-silicon (source-code level) validation of the robustness against EMFI attacks and therefore for a reasonable security assessment.
17:55 – 18:00	Closing remarks and Farewell

Wishing you a wonderful FDTC 2021!