FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Fault Diagnoses and Tolerance in Cryptography 2020

Tim Güneysu[1] **Colin O'Flynn[2]**

[1]Ruhr-University Bochum & DFKI [2]Dalhousie University

13 September, 2020 – cyberspace

Chairs

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

• Program:	**Tim Güneysu**	*Ruhr-University Bochum*
	Colin O'Flynn	*Dalhousie University*
• General:	**Guido Bertoni**	*Security Pattern*
• 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 (chair)	ENS de Paris
• Jean-Pierre Seifert	TU Berlin & T-Labs

Sponsors – Thank You!

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Program Committee

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Michel Agoyan	ST Microelectronics
Josep Balasch	KU Leuven
Lejla Batina	Radboud University
Guido Bertoni	Security Patterns
Shivam Bhasin	NTU Singapore
Luca Breveglieri	Politecnico di Milano
Ileana Buhan	Riscure
Fabrizio De Santis	SIEMENS AG
Jean-Max Dutertre	ENS Mines S. Etienne
Junfeng Fan	Open Security Research
Wieland Fischer	Infineon AG
Jorge Guajardo	Bosch US
Sylvain Guilley	Telecom ParisTech
Johann Heyszl	Fraunhofer Institute
Mehran M. Kermani	University of South Florida
Osnat Keren	Bar Ilan University

Israel Koren	University of Massachusetts
Heiko Lohrke	TU Berlin
Philippe Loubet Moundi	Gemalto
Debdeep Mukhopadhyay	IIT Kharagpur
Dmitry Nedospasov	Keylabs
David Oswald	University of Birmingham
Gerardo Pelosi	Politecnico di Milano
Ilia Polian	University of Passau
Robert Primas	TU Graz
Falk Schellenberg	Ruhr-UniversitÂ¨at Bochum
Sergei Skorobogatov	University of Cambridge
Takeshi Sugawara	UEC Tokyo
Junko Takahashi	NTT
Shahin Tajik	University of Florida
Hugues Thiebeauld	eShard
Michael Tunstall	Cryptography Research
Vincent Verneuil	NXP Semiconductors
Fan Zhang	Zhejiang University

Changes to Submission Process

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

This year is the 2nd one of "rebuttal process":

- the objective was to provide more time to allow confirmation of "fixes" to authors

- it resulted in tighter timeline (thanks to reviewers & authors!)

In cooperation with IACR

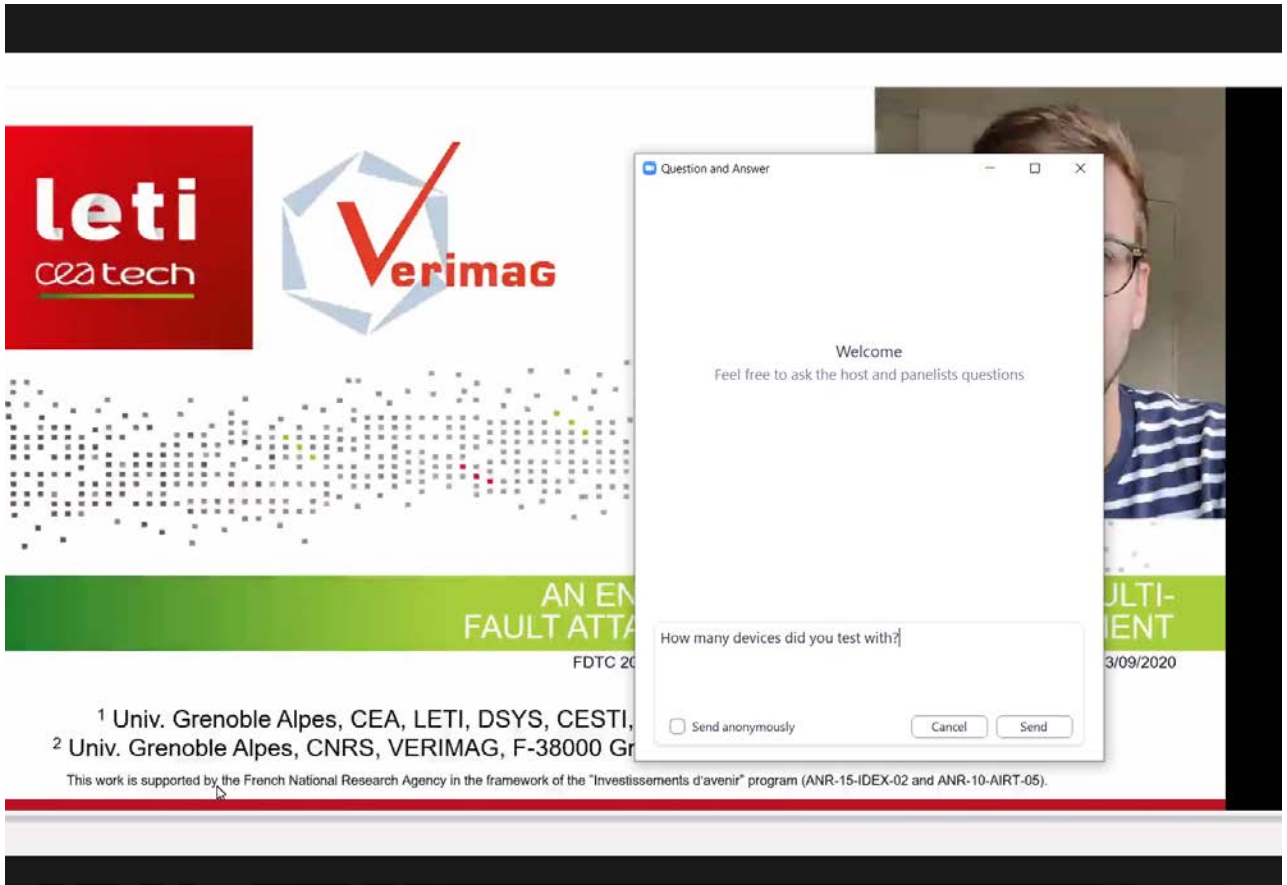
Proceedings by CS Press

Zoom Conference Notes

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

- Please use the **Q&A function** to ask questions.

- Please use the **chat function** for general conference chat.



Papers & Participants

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Submitted Papers:

- 10 papers submitted (total)
- 5 papers submitted for early (rebuttal) deadline

Accepted Papers:

- 7 accepted papers (same program size as FDTC 2019)
- 70% acceptance ratio

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

Participants to the conference: 79, from different countries.

Program Schedule – "Morning"

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Schedule refers to Central European Summer Time (CEST)

Start: 13:00 CEST (7:00 am New York – 8:00 pm Tokyo)

13:00 – 13:05 Opening remarks

Keynote Talk

Chair: Guido Bertoni

13:05 – 13:55 Faulting Hardware from Software, ***Daniel Gruss***, *Graz University of Technology*

Fault attacks induce misbehavior in a system, thereby possibly compromising the entire system and disclosing confidential data. Traditionally, fault attacks required hardware equipment and local access. In the past five years, some fault attacks have been discovered that require no local access and can instead be mounted from software. We first discuss the Rowhammer attack and how it can subvert a system. We then show that a new primitive, *Plundervolt*, can similarly lead to system compromise and information disclosure.

Daniel Gruss is Assistant Professor at the Graz University of Technology. He finished his PhD with honors in less than three years. Since 2010, he has been involved in teaching undergraduate courses on operating systems. His research focuses on side channels and security on the hardware-software boundary. His research team was involved in several vulnerability disclosures, including Meltdown and Spectre. Over the past five years, he has co-authored more than 20 top-tier academic publications and has received numerous awards for his research.

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Program Schedule – "Afternoon" 1

Session 1 – Multi-Fault Attacks *Chair: Colin O'Flynn*	
14:00 – 14:25	An End-to-End Approach for Multi-Fault Attack Vulnerability Assessment ***Vincent Werner****, Laurent Maingault and Marie-Laure Potet*
14:25 – 14:50	Countermeasures Optimization in Multiple Fault-Injection Context ***Etienne Boespflug****, Cristian Ene, Laurent Mounier and Marie-Laure Potet*
14:50 – 15:15	SPFA: SFA on Multiple Persistent Faults ***Susanne Engels****, Falk Schellenberg and Christof Paar*

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Program Schedule – "Afternoon" 2

Session 2 – Fault Injection on Primitives and Systems
Chair: Tim Güneysu

15:45 – 16:10	Attacking Hardware Random Number Generators in a Multi-Tenant Scenario *Yrjo Koyen, Adriaan Peetermans,* ***Vladimir Rozic*** *and Ingrid Verbauwhede*
16:10 – 16:35	Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation ***Menu Alexandre****, Jean-Max Dutertre, Jean-Baptiste Rigaud, Jean-Luc Danger, Brice Colombier and Pierre-Alain Moëllic*
16:35 – 17:00	Trouble at the CSIDH: Protecting CSIDH with Dummy-Operations against Fault Injection Attacks ***Fabio Campos****, Matthias J. Kannwischer, Michael Meyer, Hiroshi Onuki and Marc Stöttinger*
17:00 – 17:25	SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets ***Karim Abdellatif*** *and* ***Olivier Hériveaux***

FDTC 2020
Fault Diagnosis and Tolerance in Cryptography

Wishing you a wonderful FDTC 2020!