FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

Fault Diagnoses and Tolerance in Cryptography 2019

Johann Heyszl[1], Colin O'Flynn[2]

[1]Fraunhofer-Institute AISEC, [2]Dalhousie University

24 August, 2019 – Atlanta, Georgia, USA

Chairs

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

• Program:	**Johann Heyszl**	*Fraunhofer-Institute AISEC*
	Colin O'Flynn	*Dalhousie University*
• General:	**Guido Bertoni**	*Security Pattern*
• Publication:	**Luca Breveglieri**	*Politecnico di Milano*
• Finance:	**Israel Koren**	*University of Massachusetts*
• Local:	**David C. Keezer**	*Georgia Institute of Technology*

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 2019
Fault Diagnosis and Tolerance in Cryptography

ALPhA NOV
Optics & Lasers Technology Center

riscure
driving your security forward

Rambus

THALES

Program Committee

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

Colin O'Flynn	NewAE Technology Inc.
Johann Heyszl	Fraunhofer
Falk Schellenberg	RUB/EMSEC
Wieland Fischer	Infineon Technologies
Junfeng Fan	Open Security Research (OSR)
Luca Breveglieri	Politecnico di Milano
Patrick Schaumont	Virginia Tech
Shahin Tajik	University of Florida
Robert Primas	TUGraz
Michel Agoyan	STMicroelectronics
Philippe Loubet Moundi	Gemalto
Josep Balasch	Katholieke Universiteit Leuven
Michael Tunstall	Cryptography Research
Guido Bertoni	Security Pattern
Shivam Bhasin	Temasek Labs@NTU
Debdeep Mukhopadhyay	IIT Kharagpur, India

Hugues Thiebeauld	eShard
Lejla Batina	Radboud University
Heiko Lohrke	TU Berlin
Ileana Buhan	Riscure
David Oswald	The University of Birmingham, School of Computer Science
Jean-Max Dutertre	Ecole des Mines de Saint-Etienne
Fabrizio De Santis	Siemens AG
Fan Zhang	Zhejiang University
Mehran Mozaffari Kermani	University of South Florida
Takeshi Sugawara	The University of Electro-Communications
Ilia Polian	University of Stuttgart
Sylvain Guilley	GET/ENST, CNRS/LTCI
Vincent Verneuil	NXP Semiconductors
Israel Koren	University of Massachusetts Amherst
Gerardo Pelosi	Politecnico di Milano
Test User	University of Fun
Dmitry Nedospasov	Toothless Consulting

Changes to Submission Process

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

New “Rebuttal Process” this year.

- Objective: allow clarification between reviewers, allow authors to apply fixes / add results.

- Resulted in tighter timeline (thanks to reviewers & authors!).

In cooperation with IACR.

Proceedings by CS Press

Papers

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

Submitted Papers:

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

Accepted Papers:

- 7 accepted papers
- 58% acceptance ratio

Paper Url: https://conferences.computer.org/fdtc/2019/#!/home

Login: **fdtc19**

Password: **conf19//**

Attendees – Welcome From

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

- USA – 24
- France – 12
- Germany – 11
- Japan – 8
- Netherland – 4
- Italy – 3
- Korea, Sweden, China – 2
- Singapore, Austria, Israel, Canada - 1

Program Schedule - Morning

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

WIFI – Westin Meeting / ches2019

Session 1 – Electromagnetic Fault Injection *Chair: TBD*	
9.15 – 9:45	Precise spatio-temporal electromagnetic fault injections on data transfers *Alexandre Menu, Shivam Bhasin, Jean-Max Dutertre, Jean-Baptiste Rigaud and Jean-Luc Danger*
9:45 – 10:15	Electromagnetic fault injection: how faults occur *Mathieu Dumont, Philippe Maurine and Mathieu Lisart*
10:15 – 10:45	Morning break

Session 2 – Fault Attacks and Countermeasures *Chair: TBD*	
10:45 – 11:15	Persistent fault analysis of OCB, DEOXYS and COLM *Michael Gruber, Michael Tempelmeier and Matthias Probst*
11:15 – 11:45	Hardware-oriented algebraic fault attack framework with multiple fault injection support *Mael Gay, Tobias Paxian, Devanshi Upadhyaya, Bernd Becker and Ilia Polian*
11:45 – 12:15	Analyzing software security against complex fault models with frama-C value analysis *Johan Laurent, Christophe Deleuze, Vincent Beroulle and Florian Pebay-Peyroula*
12:15 – 13:15	Lunch

Program Schedule – Afternoon 1

FDTC 2019 Fault Diagnosis and Tolerance in Cryptography

WIFI – Westin Meeting / ches2019

Keynote Talk I *Chair: TBD*	
13:15 – 14:00	Design considerations for executing multiple distrusting applications on a secure RISCV processor *Joel Wittenauer*
Session 3 – Physical Attacks *Chair: TBD*	
14:00 – 14:30	LLFI: lateral laser fault injection attack *Joaquin Rodriguez Carunchio, Alex Baldomero Marin, Victor Montilla Gispert and Jordi Mujal*
14:30 – 15:00	RAM-jam: remote temperature and voltage fault attack on FPGAs using memory collisions *Md Mahbub Alam, Shahin Tajik, Fatemeh Ganji, Mark Tehranipoor and Domenic Forte*
15:00 – 15:30	Afternoon break

Program Schedule – Afternoon 2

FDTC 2019
Fault Diagnosis and Tolerance in Cryptography

Keynote Talk II *Chair: TBD*	
15:30 – 16:15	It's all nice, but can we trust the hardware? *Daniel Genkin*
Rump Session *Chair: TBD*	
16:15 – 16:45	for contributions use this form or contact TPC chairs
16:45 – 17:00	Closing remarks and Farewell

RUMP Submissions – Please talk to us before 1PM