FDTC 2018
Fault Diagnosis and
Tolerance in Cryptography

Fault Diagnosis and Tolerance in Cryptography 2018

Guido Bertoni[1], Joan Daemen[2] and Laurent Sauvage[3]

[1]Security Pattern [2]Radboud University [3]Télécom ParisTech

13 September 2018, Amsterdam

Organization

- Chairs:
  - General: Guido Marco Bertoni, Security Patterns
  - Publication: Luca Breveglieri, Politecnico di Milano
  - Finance: Israel Koren, University of Massachusetts
  - Local: Pedro Maat Costa Massolino, Radboud University
- Steering committee:
  - Luca Breveglieri, Politecnico di Milano
  - Israel Koren, University of Massachusetts
  - David Naccache (chair), ENS
  - Jean-Pierre Seifert, TU Berlin & T-Labs

In cooperation with IACR

Proceedings by CS Press

Sponsors

FDTC 2018
Fault Diagnosis and
Tolerance in Cryptography

ALPhA NOV
Optics & Lasers Technology Center

DARKMATTER
GUARDED BY GENIUS

Micron Foundation

Rambus

riscure
Challenge your security

POLITECNICO
MILANO

UNIVERSITY OF MASSACHUSETTS AMHERST 1863
UMASS
AMHERST

Program committee

FDTC 2018 Fault Diagnosis and Tolerance in Cryptography

Reza Azarderakhsh	Florida Atl. Univ.
Josep Balasch	KU Leuven
Shivam Bhasin	NTU Singapore
Ileana Buhan	Riscure
Rosario Cammarota	Qualcomm
Joan Daemen (**Chair**)	Radboud Univ.
Giorgio Di Natale	LIRMM
Nahid Farhady	Texas Tech. Univ.
Christophe Giraud	IDEMIA
Jorge G. Merchan	Bosch LLC
Sylvain Guilley	Telecom ParisTech
Jae Cheol Ha	Hoseo Univ.
Johann Heyszl	Fraunhofer Inst.
Michael Hutter	Rambus
Juliane Kraemer	TU Darmstadt
Victor Lomné	NinjaLabs
Philippe Maurine	Montpellier Univ.
Philippe Loubet Moundi	Gemalto
Mehran M. Kermani	Rochester Inst. Tech.
Debdeep Mukhopadhyay	IIT Kharagpur
David Oswald	Univ. Birmingham
Gerardo Pelosi	Politec. Milano
Ilia Polian	Univ. of Passau
Arash Reyhani	Univ. West. Ontario
Francesco Regazzoni	Alari - USI
Laurent Sauvage (**Chair**)	Telecom ParisTech
Patrick Schaumont	Virginia Tech
Joern-Marc Schmidt	Secunet
Jean-Pierre Seifert	TU Berlin & T-Labs
Sergei Skorobogatov	Univ. Cambridge
Takeshi Sugawara	UEC Tokyo
Junko Takahashi	NTT Laboratories
Michael Tunstall	Rambus
Vincent Verneuil	NXP Semiconductors
Qiaoyan Yu	Univ. New Hampshire

Papers

- Submitted papers:
  - 12 papers submitted
  - 35 committee members
  - 3 reviews per paper
  - 1 review per committee member
- Accepted papers
  - 7 papers accepted
  - 58 % acceptance ratio
  - 46 co-authors in total
  - almost 7 authors per paper

Proceedings at `http://euler.ecs.umass.edu/FDTC/`
(password: amsterdam)

Wifi password: FDTC2018

126 participants

- France 24
- Germany 23
- USA 20
- China 11
- The Netherlands 9
- Belgium 6
- Japan 6
- Spain 4
- Switzerland 4
- Italy 3
- South Korea 3
- United Kingdom 3
- Singapore 2
- Sweden 2
- Austria 1
- Canada 1
- Croatia 1
- India 1
- Israel 1
- Russia 1

Program, morning

FDTC 2018
Fault Diagnosis and
Tolerance in Cryptography

8:45	Registration
9:05	Opening remarks
Session 1: Laser Fault Attacks, Chair Laurent Sauvage	
9.15	Laser fault injection at CMOS 28 nm: analysis of fault model J. Dutertre, V. Beroulle, S. De Castro, L. Faber, M. Flottes, P. Gendrier, D. Hely, R. Leveugle, P. Maistri, G. Di Natale, A. Papadimitriou and B. Rouzeyre
9:45	Latch-up-locked? – empirical study on ARM Cortex-M laser faults B. Selmke, K. Zinnecker, P. Koppermann, K. Miller, J. Heyszl & G. Sigl
10:15	Morning break
Session 2: Fault Attacks and Countermeasures, Chair Begül Bilgin	
10:45	Breaking redundancy with random faults and power side channel S. Saha, S. Bhasin, D. Jap, J. Breier, D. Mukhopadhyay and P. Dasgupta
11:15	Darth's saber: laser key exfiltration for symmetric ciphers G. Bertoni, V. Zaccaria, M. Molteni and F. Melzani
11:45	Glitch-resistant masking schemes against fault sensitivity analysis, Victor Arribas, Thomas De Cnudde and Danilo Sijacic
12:15	Lunch

Program, afternoon

12:15	Lunch
Session 3: Electromagnetic Fault Attacks, Chair Elif Bilge Kavun	
13:15	Genetic algorithm-based electromagnetic fault injection, A. Maldini, N. Samwel, S. Picek & L. Batina
13:45	The impact of pulsed electromagnetic fault injection on TRNG, M. Madau, M. Agoyan, J. Balash, M. Grujic, P. Haddad, P. Maurine, V. Rozic, D. Singelee, I. Verbauwhede & B. Yang
Keynote talk, Chair Joan Daemen	
14:15	The SP800-90B approach to entropy sources, John Kelsey
15:05	Afternoon break
Panel discussion, Moderator Guido Bertoni	
15:35	Random generator testing and evaluation, Panel: John Kelsey, Sylvain Guilley, Assia Tria, Werner Schindler
16:50	Closing remarks and Farewell