

2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2018)

**Amsterdam, Netherlands
13 September 2018**



**IEEE Catalog Number: CFP1886C-POD
ISBN: 978-1-5386-8198-5**

**Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1886C-POD
ISBN (Print-On-Demand):	978-1-5386-8198-5
ISBN (Online):	978-1-5386-8197-8

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2018 Workshop on Fault Diagnosis and Tolerance in Cryptography **FDTC 2018**

Table of Contents

Preface	vii
Conference Organization	viii
Program Committee	ix
Acknowledgments	x

Session 1: Laser Fault Attacks

Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model	1
<i>Jean-Max Dutertre (Mines Saint-Etienne, CEA Tech, Centre CMP), Vincent Beroulle (Univ. Grenoble Alpes, Grenoble INP, LCIS), Philippe Candelier (STMicroelectronics), Stephan De Castro (LIRMM, University of Montpellier, CNRS), Louis-Barthelemy Faber (STMicroelectronics), Marie-Lise Flottes (LIRMM, University of Montpellier, CNRS), Philippe Gendrier (STMicroelectronics), David Hély (Univ. Grenoble Alpes, Grenoble INP, LCIS), Regis Leveugle (Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA), Paolo Maistri (Univ. Grenoble Alpes, CNRS, Grenoble INP, TIMA), Giorgio Di Natale (LIRMM, University of Montpellier, CNRS), Athanasios Papadimitriou (Univ. Grenoble Alpes, Grenoble INP, LCIS), and Bruno Rouzeyre (LIRMM, University of Montpellier, CNRS)</i>	
Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors	7
<i>Bodo Selmke (Fraunhofer Research Institution AISEC), Kilian Zinnecker (Fraunhofer Research Institution AISEC), Philipp Koppermann (Fraunhofer Research Institution AISEC), Katja Miller (Fraunhofer Research Institution AISEC), Johann Heyszl (Fraunhofer Research Institution AISEC), and Georg Sigl (Technische Universität München, EISEC)</i>	

Session 2: Fault Attacks and Countermeasures

Breaking Redundancy-Based Countermeasures with Random Faults and Power Side Channel	15
<i>Sayandeep Saha (IIT Kharagpur), Dirmanto Jap (Nanyang Technological University), Jakub Breier (Nanyang Technological University), Shivam Bhasin (Nanyang Technological University), Debdeep Mukhopadhyay (IIT Kharagpur), and Pallab Dasgupta (IIT Kharagpur)</i>	

Darth's Saber: A Key Exfiltration Attack for Symmetric Ciphers Using Laser Light .23.....	
<i>Vittorio Zaccaria (Politecnico di Milano), Maria Chiara Molteni</i>	
<i>(Politecnico di Milano), Filippo Melzani (Security Pattern), and Guido</i>	
<i>Bertoni (Security Pattern)</i>	
Glitch-Resistant Masking Schemes as Countermeasure Against Fault Sensitivity Analysis .27.....	
<i>Victor Arribas (imec-COSIC, KU Leuven), Thomas De Cnudde (imec-COSIC,</i>	
<i>KU Leuven), and Danilo Šijai (imec-COSIC, KU Leuven)</i>	

Session 3: Electromagnetic Fault Attacks

Genetic Algorithm-Based Electromagnetic Fault Injection .35.....	
<i>Antun Maldini (Faculty of Electrical Engineering and Computing,</i>	
<i>University of Zagreb), Niels Samwel (Digital Security Group, Radboud</i>	
<i>University), Stjepan Picek (Cyber Security Research Group, Delft</i>	
<i>University of Technology), and Lejla Batina (Digital Security Group,</i>	
<i>Radboud University)</i>	
The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators .43.....	
<i>Maxime Madau (STMicroelectronics), Michel Agoyan (STMicroelectronics),</i>	
<i>Josep Balasch (COSIC KU Leuven), Miloš Grujić (COSIC KU Leuven),</i>	
<i>Patrick Haddad (STMicroelectronics), Philippe Maurine (Laboratoire</i>	
<i>d'Informatique, de Robotique et de Microelectronique de Montpellier),</i>	
<i>Vladimir Roži (COSIC, KU Leuven), Dave Singelée (COSIC, KU Leuven),</i>	
<i>Bohan Yang (COSIC, KU Leuven), and Ingrid Verbauwhede (COSIC, KU</i>	
<i>Leuven)</i>	

Panel Contribution

Random Numbers Generation: Tests and Attacks .49.....	
<i>Sylvain Guilley (Secure-IC S.A.S.; LTCI, Telecom ParisTech; Ecole</i>	
<i>Normale Supérieure) and Youssef El Housni (Secure-IC)</i>	

Author Index 55.....	
----------------------	--