

2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2022)

**Virtual Workshop
16 September 2022**



IEEE Catalog Number: CFP2286C-POD
ISBN: 978-1-6654-5443-8

**Copyright © 2022 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:	CFP2286C-POD
ISBN (Print-On-Demand):	978-1-6654-5443-8
ISBN (Online):	978-1-6654-5442-1

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

2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) **FDTC 2022**

Table of Contents

Preface	vii
Organizing Committee	ix
Program Committee	x
Keynote Message	xi
Sponsors	xiii

Laser-Based Fault Attacks

Embedded-EEPROM Descrambling via Laser-Based Techniques – A Case Study on AVR MCU .. 1 <i>Samuel Chef (Nanyang Technological University, Singapore), Chung Tah Chua (Nanyang Technological University, Singapore), Jing Yun Tay (Nanyang Technological University, Singapore), Jason Cheah (Nanyang Technological University, Singapore), and Chee Lip Gan (Nanyang Technological University, Singapore)</i>	
Triple Exploit Chain with Laser Fault Injection on a Secure Element	9
<i>Olivier Hériveaux (Ledger)</i>	
The More You Know: Improving Laser Fault Injection with Prior Knowledge	18
<i>Marina Krček (TU Delft), Thomas Ordas (STMicroelectronics), Daniele Fronte (STMicroelectronics), and Stjepan Picek (Radboud University)</i>	

Fault Attacks to Public Key Cryptosystems

FA-LLing for RSA: Lattice-Based Fault Attacks against RSA Encryption and Signature	30
<i>Guillaume Barbu (IDEMIA, France)</i>	
Generalising Fault Attacks to Genus Two Isogeny Cryptosystems	38
<i>Ariana Goh (DSO National Laboratories, Singapore), Chu-Wee Lim (DSO National Laboratories, Singapore), and Yan Bo Ti (DSO National Laboratories, Singapore)</i>	

Fault Injection: Techniques, Analysis, Effects

Body Biasing Injection: Impact of Substrate Types on the Induced Disturbances?	50
<i>Geoffrey Chancel (Université de Montpellier, LIRMM), Jean-Marc Gallière (Université de Montpellier, LIRMM), and Philippe Maurine (Université de Montpellier, LIRMM)</i>	

Quantifying the Speed-Up Offered by Genetic Algorithms during Fault Injection	
Cartographies	61
<i>Idris Rais-Ali (Secure-IC S.A.S), Antoine Bouvet (Secure-IC S.A.S),</i>	
<i>and Sylvain Guilley (Secure-IC S.A.S / Telecom Paris)</i>	
Exploration of Fault Effects on Formal RISC-V Microarchitecture Models	73
<i>Simon Tollec (Université Paris-Saclay, CEA, France), Mihail Asavoae</i>	
<i>(Université Paris-Saclay, CEA, France), Damien Couroussé (Université</i>	
<i>Grenoble Alpes, CEA, France), Karine Heydemann (Sorbonne Université,</i>	
<i>CNRS, France), and Mathieu Jan (Université Paris-Saclay, CEA, France)</i>	
Author Index	85