

2020 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2020)

**Milan, Italy
13 September 2020**



**IEEE Catalog Number: CFP2086C-POD
ISBN: 978-1-7281-9563-6**

**Copyright © 2020 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:	CFP2086C-POD
ISBN (Print-On-Demand):	978-1-7281-9563-6
ISBN (Online):	978-1-7281-9562-9

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

2020 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) **FDTC 2020**

Table of Contents

Preface	vi
Program Committee	vii
Acknowledgments	viii
Contact Information	ix
An End-to-End Approach for Multi-Fault Attack Vulnerability Assessment	10
<i>Vincent Werner (Univ. Grenoble Alpes, CEA, LETI, DSYS, CESTI), Laurent Maingault (Univ. Grenoble Alpes, CEA, LETI, DSYS, CESTI), and Marie-Laure Potet (Univ. Grenoble Alpes, CNRS, VERIMAG)</i>	
Attacking Hardware Random Number Generators in a Multi-Tenant Scenario	18
<i>Yrjo Koyen (KU Leuven), Adriaan Peetermans (KU Leuven), Vladimir Rozic (KU Leuven), and Ingrid Verbauwhede (KU Leuven)</i>	
Countermeasures Optimization in Multiple Fault-Injection Context	26
<i>Etienne Boespflug (University of Grenoble-Alpes), Cristian Ene (University of Grenoble-Alpes), Laurent Mounier (University of Grenoble-Alpes), and Marie-Laure Potet (University of Grenoble-Alpes)</i>	
SiliconToaster: A Cheap and Programmable EM Injector for Extracting Secrets	35
<i>Karim M. Abdellatif (Ledger) and Olivier Hériveaux (Ledger)</i>	
Single-bit Laser Fault Model in NOR Flash Memories: Analysis and Exploitation	41
<i>Alexandre Menu (Mines Saint-Etienne), Jean-Max Dutertre (Mines Saint-Etienne), Jean-Baptiste Rigaud (Mines Saint-Etienne), Brice Colombier (UJM Saint-Etienne), Pierre-Alain Moellic (CEA-TECH Mines Saint-Etienne), and Jean-Luc Danger (Télécom Paris)</i>	
SPFA: SFA on Multiple Persistent Faults	49
<i>Susanne Engels (Max Planck Institute for Security and Privacy, Ruhr University Bochum), Falk Schellenberg (Max Planck Institute for Security and Privacy), and Christof Paar (Max Planck Institute for Security and Privacy)</i>	
Trouble at the CSIDH: Protecting CSIDH with Dummy-Operations Against Fault Injection Attacks	57
<i>Fabio Campos (University of Applied Sciences Wiesbaden), Matthias J. Kannwischer (Radboud University), Michael Meyer (University of Applied Sciences Wiesbaden, University of Würzburg), Hiroshi Onuki (University of Tokyo), and Marc Stöttinger (Continental AG)</i>	
Author Index	67