

# **2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2021)**

**Virtual Workshop  
17 September 2021**



**IEEE Catalog Number: CFP2186C-POD  
ISBN: 978-1-6654-3674-8**

**Copyright © 2021 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:	CFP2186C-POD
ISBN (Print-On-Demand):	978-1-6654-3674-8
ISBN (Online):	978-1-6654-3673-1

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) **FDTC 2021**

## Table of Contents

Preface	vii
Organizing Committee	ix
Program Committee	x
Keynotes	xii
Panel Discussion	xiii
Sponsors	xiv

### Fault Analysis

On the Importance of Initial Solutions Selection in Fault Injection	1
<i>Marina Krcek (Delft University of Technology, The Netherlands), Daniele Fronte (STMicroelectronics, France), and Stjepan Picek (Delft University of Technology, The Netherlands)</i>	
A High-Order Infective Countermeasure Framework	13
<i>Guillaume Barbu (IDEMIA, France), Luk Bettale (IDEMIA, France), Laurent Castelnovi (IDEMIA, France), Thomas Chabrier (IDEMIA, France), Nicolas Debande (IDEMIA, France), Christophe Giraud (IDEMIA, France), and Nathan Reboud (IDEMIA, France)</i>	
ARCHIE: A QEMU-Based Framework for Architecture-Independent Evaluation of Faults	20
<i>Florian Hauschild (Technical University of Munich, Germany), Kathrin Garb (Fraunhofer Institute AISEC, Germany), Lukas Auer (Fraunhofer Institute AISEC, Germany), Bodo Selmke (Fraunhofer Institute AISEC, Germany), and Johannes Obermaier (n/a)</i>	
EM Fault Model Characterization on SoCs: From Different Architectures to the Same Fault Model	31
<i>Thomas Troughkine (National Cybersecurity Agency of France (ANSSI), France), Guillaume Bouffard (National Cybersecurity Agency of France (ANSSI), France, PSL University, France), and Jessy Clédière (CEA, LETI, MINATEC Campus, France)</i>	

### Short Presentations

Safe-Error Analysis of Post-Quantum Cryptography Mechanisms	39
<i>Luk Bettale (IDEMIA, France), Simon Montoya (IDEMIA, France, LIX, INRIA, CNRS, École Polytechnique, IPP, France), and Guénaél Renault (ANSSI, France, LIX, INRIA, CNRS, École Polytechnique, IPP, France)</i>	

Algebraic Fault Analysis of Subterranean 2.0 .45.....  
*Michael Gruber (Technical University of Munich, Chair of Security in Information Technology, Germany), Patrick Karl (Technical University of Munich, Chair of Security in Information Technology, Germany), and Georg Sigl (Technical University of Munich, Chair of Security in Information Technology, Germany, Fraunhofer Institute for Applied and Integrated Security, Germany)*

Are Cold Boot Attacks Still Feasible: A Case Study on Raspberry Pi With Stacked Memory .56.....  
*Yoo-Seung Won (Temasek Laboratories at Nanyang Technological University, Singapore) and Shivam Bhasin (Temasek Laboratories at Nanyang Technological University, Singapore)*

EMFI for Safety-Critical Testing of Automotive Systems .61.....  
*Colin O’Flynn (Dalhousie University, Canada)*

## Experimentation on Fault Attacks

On the Scaling of EMFI Probes .67.....  
*Julien Toulemont (University of Montpellier, LIRMM, France), Geoffrey Chancel (University of Montpellier, LIRMM, France), Jean-Marc Galliere (University of Montpellier, LIRMM, France), Frederick Mailly (University of Montpellier, LIRMM, France), Pascal Nouet (University of Montpellier, LIRMM, France), and Philippe Maurine (University of Montpellier, LIRMM, France)*

Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline .74.....  
*Vanthanh Khuat (LTCI, Télécom Paris, Institut polytechnique de Paris, France, Le Quy Don Technical University, Vietnam), Jean-luc Danger (LTCI, Télécom Paris, Institut polytechnique de Paris, France), and Jean-Max Dutertre (Mines Saint-Etienne, CEA, Leti, Centre CMP, France)*

The Forgotten Threat of Voltage Glitching: A Case Study on Nvidia Tegra X2 SoCs .86.....  
*Otto Bittner (Technische Universität Berlin), Thilo Krachenfels (Technische Universität Berlin), Andreas Galauner (Independent Researcher), and Jean-Pierre Seifert (Technische Universität Berlin, Fraunhofer SIT)*

**Author Index 99**.....