

# **2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2019)**

**Atlanta, Georgia, USA  
24 August 2019**



**IEEE Catalog Number: CFP1986C-POD  
ISBN: 978-1-7281-3823-7**

**Copyright © 2019 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:    | CFP1986C-POD      |
| ISBN (Print-On-Demand): | 978-1-7281-3823-7 |
| ISBN (Online):          | 978-1-7281-2667-8 |

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

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) FDTC 2019

## Table of Contents

|                                     |  |
|-------------------------------------|--|
| <b>Preface</b> .vii.....            |  |
| <b>Program Committee</b> .viii..... |  |
| <b>Acknowledgments</b> .ix.....     |  |
| <b>Contact Information</b> .x.....  |  |

### Session 1: Electromagnetic Fault Injection

|   |  |
|---|--|
| Precise Spatio-Temporal Electromagnetic Fault Injections on Data Transfers .1.....  |  |
| <i>Alexandre Menu (Mines Saint-Etienne, CEA-Tech, Centre CMP, France),<br/>Shivam Bhasin (Nanyang Technological University, Singapore), Jean-Max<br/>Dutertre (Mines Saint-Etienne, CEA-Tech, Centre CMP, France),<br/>Jean-Baptiste Rigaud (Mines Saint-Etienne, CEA-Tech, Centre CMP,<br/>France), and Jean-Luc Danger (LTCI, Télécom ParisTech, Institut<br/>Mines-télécom, Université Paris Saclay, France)</i> |  |
| Electromagnetic Fault Injection : How Faults Occur .9.....  |  |
| <i>Mathieu Dumont (STMicroelectronics, LIRMM), Mathieu Lisart<br/>(STMicroelectronics), and Philippe Maurine (LIRMM)</i>  |  |

### Session 2: Fault Attacks and Countermeasures

|   |  |
|---|--|
| Persistent Fault Analysis of OCB, DEOXYS and COLM .17.....  |  |
| <i>Michael Gruber (Technical University of Munich), Matthias Probst<br/>(Technical University of Munich), and Michael Tempelmeier (Technical<br/>University of Munich)</i>  |  |
| Hardware-Oriented Algebraic Fault Attack Framework with Multiple Fault Injection Support .25.....   |  |
| <i>Maël Gay (University of Stuttgart), Tobias Paxian (University of<br/>Freiburg), Devanshi Upadhyaya (University of Stuttgart), Bernd Becker<br/>(University of Freiburg), and Ilia Polian (University of Stuttgart)</i>   |  |
| Analyzing Software Security Against Complex Fault Models with Frama-C Value Analysis .33.....   |  |
| <i>Johan Laurent (Univ. Grenoble Alpes, Grenoble INP, LCIS), Christophe<br/>Deleuze (Univ. Grenoble Alpes, Grenoble INP, LCIS), Vincent Beroulle<br/>(Univ. Grenoble Alpes, Grenoble INP, LCIS), and Florian Pebay-Peyroula<br/>(Univ. Grenoble Alpes, CEA, LETI)</i> |  |

## Session 3: Physical Attacks

|   |    |
|---|----|
| LLFI: Lateral Laser Fault Injection Attack .41.....   | 41 |
| <i>Joaquin Rodriguez (Applus+ Laboratories), Alex Baldomero (Applus+ Laboratories), Victor Montilla (Applus+ Laboratories), and Jordi Mujal (Applus+ Laboratories)</i>  |    |
| RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions .48.....  | 48 |
| <i>Md Mahbub Alam (University of Florida), Shahin Tajik (University of Florida), Fatemeh Ganji (University of Florida), Mark Tehranipoor (University of Florida), and Domenic Forte (University of Florida)</i> |    |
| <b>Author Index</b> 57.....   | 57 |