

# **2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2017)**

**Taipei, Taiwan  
25 September 2017**



**IEEE Catalog Number: CFP1786C-POD  
ISBN: 978-1-5386-2949-9**

**Copyright © 2017 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:	CFP1786C-POD
ISBN (Print-On-Demand):	978-1-5386-2949-9
ISBN (Online):	978-1-5386-2948-2

**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

# 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography

## FDTC 2017

### Table of Contents

Preface.....	vii
Workshop Organization .....	viii
Program Committee.....	ix
Additional Reviewers.....	x
Acknowledgements .....	xi

---

#### System-Level Fault Attacks

Escalating Privileges in Linux Using Voltage Fault Injection .....	1
<i>Niek Timmers and Cristofaro Mune</i>	
Safety != Security: On the Resilience of ASIL-D Certified Microcontrollers against Fault Injection Attacks .....	9
<i>Nils Wiersma and Ramiro Pareja</i>	

#### Fault Attacks on Primitives

Practical Fault Attack against the Ed25519 and EdDSA Signature Schemes .....	17
<i>Yolan Romailer and Sylvain Pelissier</i>	
One Plus One is More than Two: A Practical Combination of Power and Fault Analysis Attacks on PRESENT and PRESENT-Like Block Ciphers .....	25
<i>Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, and Shivam Bhasin</i>	
A Practical Fault Attack on ARX-Like Ciphers with a Case Study on ChaCha20 .....	33
<i>S. V. Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay, and Anubhab Baksi</i>	

## **Laser Fault Attacks**

Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot .....	41
<i>Aurélien Vasselle, Hugues Thiebauld, Quentin Maouhoub, Adèle Morisset, and Sébastien Ermenoux</i>	
Exploiting Bitflip Detector for Non-invasive Probing and its Application to Ineffective Fault Analysis .....	49
<i>Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, and Makoto Nagata</i>	

## **Design Tools**

CAMFAS: A Compiler Approach to Mitigate Fault Attacks via Enhanced SIMDization .....	57
<i>Zhi Chen, Junjie Shen, Alex Nicolau, Alex Veidenbaum, Nahid Farhady Ghalaty, and Rosario Cammarota</i>	
AutoFault: Towards Automatic Construction of Algebraic Fault Attacks .....	65
<i>Jan Burchard, Maël Gay, Ange-Salomé Messeng Ekossono, Jan Horáček, Bernd Becker, Tobias Schubert, Martin Kreuzer, and Ilia Polian</i>	
<b>Author Index</b> .....	73