

2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2016)

**Santa Barbara, California, USA
16 August 2016**



**IEEE Catalog Number: CFP1686C-POD
ISBN: 978-1-5090-1109-4**

**Copyright © 2016 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 publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1686C-POD
ISBN (Print-On-Demand):	978-1-5090-1109-4
ISBN (Online):	978-1-5090-1108-7

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

2016 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2016

Table of Contents

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

Invited Paper I

Attacks on Encrypted Memory and Constructions for Memory Protection	1
<i>Shay Gueron</i>	

Differential Fault Analysis

Differential Fault Analysis of SHA3-224 and SHA3-256	4
<i>Pei Luo, Yunsu Fei, Liwei Zhang, and A. Adam Ding</i>	
Improved Fault Analysis on SIMON Block Cipher Family	16
<i>Hua Chen, Jingyi Feng, Vincent Rijmen, Yunwen Liu, Limin Fan, and Wei Li</i>	

Fault Injection-Based Attacks

Controlling PC on ARM Using Fault Injection	25
<i>Niek Timmers, Albert Spruyt, and Marc Witteman</i>	
Attack on a DFA Protected AES by Simultaneous Laser Fault Injections	36
<i>Bodo Selmke, Johann Heyszl, and Georg Sigl</i>	
Software Fault Resistance is Futile: Effective Single-Glitch Attacks	47
<i>Bilgidey Yuze, Nahid Farhady Ghalaty, Harika Santapuri, Chinmay Deshpande, Conor Patrick, and Patrick Schaumont</i>	

Invited Paper II

Continuous-Time Computational Aspects of Cyber-Physical Security	59
<i>Sam Green, İhsan Çiçek, and Çetin Kaya Koç</i>	

Fault Sensitivity and Fault Detection

Lattice-Based Signature Schemes and Their Sensitivity to Fault Attacks	63
<i>Nina Bindel, Johannes Buchmann, and Juliane Krämer</i>	
An Embedded Digital Sensor against EM and BB Fault Injection	78
<i>David El-Baze, Jean-Baptiste Rigaud, and Philippe Maurine</i>	

Countermeasures against Fault Injection-Based Attacks

Fault Tolerant Implementations of Delay-Based Physically Unclonable Functions on FPGA	87
<i>Durga Prasad Sahoo, Sikhar Patranabis, Debdeep Mukhopadhyay, and Rajat Subhra Chakraborty</i>	
Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection	102
<i>Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, and Makoto Nagata</i>	
More Efficient Private Circuits II through Threshold Implementations	114
<i>Thomas de Cnudde and Svetla Nikova</i>	
Author Index	125