

2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2015)

**Saint Malo, France
13 September 2015**



**IEEE Catalog Number: CFP1586C-POD
ISBN: 978-1-4673-7580-1**

**Copyright © 2015 by the Institute of Electrical and Electronic 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:	CFP1586C-POD
ISBN (Print-On-Demand):	978-1-4673-7580-1
ISBN (Online):	978-1-4673-7579-5

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

2015 Workshop on Fault Diagnosis and Tolerance in Cryptography

FDTC 2015

Table of Contents

Preface.....	vii
Program Committee.....	viii
Additional Reviewers.....	ix
Acknowledgments.....	x
Organizers' Contact Information.....	xi

Invited Papers

Fault Attacks at the System Level - The Challenge of Securing Application Software	1
<i>Stefan Mangard</i>	
The Need for Intrinsic Hardware Security Below 65nm	2
<i>Mathias Wagner</i>	

Session 1: Fault Injection: Models and Techniques

EM Injection: Fault Model and Locality	3
<i>S. Ordas, L. Guillaume-Sage, and Philippe Maurine</i>	
On the Complexity Reduction of Laser Fault Injection Campaigns Using OBIC Measurements	14
<i>Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schäpers, Nils Gerhardt, Martin Hofmann, and Christof Paar</i>	

Session 2: DFA: Models and Techniques

Improved Differential Fault Attack on the Block Cipher SPECK	28
<i>Yuming Huo, Fan Zhang, Xiutao Feng, and Li-Ping Wang</i>	
J-DFA: A Novel Approach for Robust Differential Fault Analysis	35
<i>Luca Magri, Silvia Mella, Pasqualina Fragneto, Filippo Melzani, and Beatrice Rossi</i>	

Lost in Translation: Fault Analysis of Infective Security Proofs	45
<i>Alberto Battistello and Christophe Giraud</i>	

Session 3: Fault Injection Attacks to Cipher Families

To Exploit Fault Injection on Non-injective Sboxes	54
<i>Guillaume Bethouart and Nicolas Debande</i>	
An Efficient One-Bit Model for Differential Fault Analysis on Simon Family	61
<i>Juan del Carmen Grados Vásquez, Fábio Borges, Renato Portugal, and Pedro Lara</i>	

Session 4: Fault Attacks to Cryptographic Devices

Singular Curve Point Decompression Attack	71
<i>Johannes Blömer and Peter Günther</i>	
Laser Fault Attack on Physically Unclonable Functions	85
<i>Shahin Tajik, Heiko Lohrke, Fatemeh Ganji, Jean-Pierre Seifert, and Christian Boit</i>	
Improving Fault Attacks on Embedded Software Using RISC Pipeline Characterization	97
<i>Bilgiday Yuce, Nahid Farhady Ghalaty, and Patrick Schaumont</i>	

Author Index	109
---------------------------	-----