

2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2023)

**Prague, Czech Republic
10 September 2023**



**IEEE Catalog Number: CFP2386C-POD
ISBN: 979-8-3503-4253-6**

**Copyright © 2023 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:	CFP2386C-POD
ISBN (Print-On-Demand):	979-8-3503-4253-6
ISBN (Online):	979-8-3503-4252-9
ISSN:	2995-0244

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

2023 Workshop on Fault Detection and Tolerance in Cryptography (FDTC) **FDTC 2023**

Table of Contents

Preface	vii
Organizing Committee	ix
Program Committee	x
Sponsors	xi
Keynote	xii

Fault Attack Models and Countermeasures

A Tale of Two Models: Discussing the Timing and Sampling EM Fault Injection Models	1
<i>Roukoz Nabhan (Mines Saint-Etienne, France), Jean-Max Dutertre (Mines Saint-Etienne, France), Jean-Baptiste Rigaud (Mines Saint-Etienne, France), Jean-Luc Danger (Télécom Paris, France), and Laurent Sauvage (Télécom Paris, France)</i>	
Voronoi Based Multidimensional Parameter Optimization for Fault Injection Attacks	13
<i>Marius Eggert (RheinMain University of Applied Sciences, Germany) and Marc Stöttinger (RheinMain University of Applied Sciences, Germany)</i>	
A Compositional Methodology to Harden Programs against Multi-fault Attacks	24
<i>Etienne Boespflug (VERIMAG, Université Grenoble Alpes, France), Laurent Mounier (VERIMAG, Université Grenoble Alpes, France), Marie-Laure Potet (VERIMAG, Université Grenoble Alpes, France), and Abderrahmane Bouguern (VERIMAG, Université Grenoble Alpes, France)</i>	

Fault Injection Analysis and Tools

Analysis of Arbitrary Waveform Generation for Voltage Glitches	36
<i>Stanislav Lyakhov (Oregon State University, USA) and Vincent Immler (Oregon State University, USA)</i>	
A Better Practice for Body Biasing Injection	48
<i>Geoffrey Chancel (LIRMM - University of Montpellier, France), Jean-Marc Gallière (LIRMM - University of Montpellier, France), and Philippe Maurine (LIRMM - University of Montpellier, France)</i>	
PicoEMP: A Low-Cost EMFI Platform Compared to BBI and Voltage Fault Injection Using TDC and External VCC Measurements	60
<i>Colin O'Flynn (Dalhousie University, Canada)</i>	

Fault Attacks on SW and HW Devices

Fault Attacks on a Cloud-Assisted ECDSA White-Box Based on the Residue Number System	72
<i>Christophe Giraud (IDEMIA Cryptography and Security Labs, France) and Agathe Houzelot (IDEMIA Cryptography and Security Labs, France; LaBRI, CNRS, Université de Bordeaux, France)</i>	
Forging DILITHIUM and FALCON Signatures by Single Fault Injection	81
<i>Sven Bauer (Siemens AG, Technology, Germany) and Fabrizio De Santis (Siemens AG, Technology, Germany)</i>	
DeepCover DS28C36: A Hardware Vulnerability Identification and Exploitation Using T-Test and Double Laser Fault Injection	89
<i>Karim M. Abdellatif (Ledger, Donjon) and Olivier Hériveaux (Ledger, Donjon)</i>	
Author Index	95