2024 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2024)

Halifax, Nova Scotia, Canada
4 September 2024

IEEE

IEEE Catalog Number: CFP2486C-POD
ISBN: 979-8-3503-8037-8

****** 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:	CFP2486C-POD
ISBN (Print-On-Demand):	979-8-3503-8037-8
ISBN (Online):	979-8-3503-8036-1
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

2024 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)

FDTC 2024

Table of Contents

Preface ..... **vii**
Organizing Committee ..... **ix**
Program Committee ..... **x**
Keynotes ..... **xi**
Sponsors ..... **xiii**

FDTC 2024

Improving CPU Fault Injection Simulations: Insights from RTL to Instruction-Level Models 1
Jasper Van Woudenberg (Riscure, San Francisco, USA), Rajesh Velegalati (Riscure, San Francisco, USA), Cees-Bart Breunesse (Riscure, San Francisco, USA), and Dennis Vermoen (Riscure, San Francisco, USA)

PoP DRAM: A new EMFI Approach Based on EM-Induced Glitches on SoC 10
Clément Fanjas (CEA-Tech, Centre CMP, Équipe Commune CEA Tech - Mines Saint-Étienne, France; Université Grenoble Alpes, CEA, Leti, France), Driss Aboulkassimi (CEA-Tech, Centre CMP, Équipe Commune CEA Tech - Mines Saint-Étienne, France; Université Grenoble Alpes, CEA, Leti, France), Simon Pontié (CEA-Tech, Centre CMP, Équipe Commune CEA Tech - Mines Saint-Étienne, France; Université Grenoble Alpes, CEA, Leti, France), and Jessy Clédière (CEA-Leti, 17 av. Des Martyrs, France)

Switch-Glitch: Location of Fault Injection Sweet Spots by Electro-Magnetic Emanation 22
Matthias Probst (Technical University of Munich, Germany), Michael Gruber (Technical University of Munich, Germany), Manuel Brosch (Technical University of Munich, Germany), Tim Music (Technical University of Munich, Germany), and Georg Sigl (Technical University of Munich, Germany)

MAYo or MAY-not: Exploring Implementation Security of the Post-Quantum Signature Scheme MAYO Against Physical Attacks 28
Thomas Aulbach (University of Regensburg, Germany), Soundes Marzougui (STMicroelectronics, Belgium), Jean-Pierre Seifert (TU Berlin — SECT, Germany; Fraunhofer SIT, Germany), and Vincent Quentin Ulitzsch (TU Berlin — SECT, Germany)

A Single-Trace Fault Injection Attack on Hedged Module Lattice Digital Signature Algorithm (ML-DSA) 34
Sönke Jendral (KTH Royal Institute of Technology, Sweden), John Preuß Mattsson (Ericsson Research, Sweden), and Elena Dubrova (KTH Royal Institute of Technology, Sweden)

Fault Injection Attacks Exploiting High Voltage Pulsing over Si-Substrate Backside of IC Chips 44
Yusuke Hayashi (Kobe University, Japan), Rikuu Hasegawa (Kobe University, Japan), Takuya Wadatsumi (Kobe university, Japan), Kazuki Monta (Kobe University, Japan), Takuji Miki (Kobe University, Japan), and Makoto Nagata (Kobe University, Japan)

FaultyGarble: Fault Attack on Secure Multiparty Neural Network Inference 53
Mohammad Hashemi (Worcester Polytechnic Institute), Dev Mehta (Worcester Polytechnic Institute), Kyle Mitard (Worcester Polytechnic Institute), Shahin Tajik (Worcester Polytechnic Institute), and Fatemeh Ganji (Worcester Polytechnic Institute)

Author Index **65**