# 2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2022)

## Virtual Workshop
## 16 September 2022

IEEE

**IEEE Catalog Number:** CFP2286C-POD
**ISBN:** 978-1-6654-5443-8

****** 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: | CFP2286C-POD |
| ISBN (Print-On-Demand): | 978-1-6654-5443-8 |
| ISBN (Online): | 978-1-6654-5442-1 |

**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

# 2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)

# FDTC 2022

## Table of Contents

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

### Laser-Based Fault Attacks

Embedded-EEPROM Descrambling via Laser-Based Techniques – A Case Study on AVR MCU .. 1
*Samuel Chef (Nanyang Technological University, Singapore), Chung Tah Chua (Nanyang Technological University, Singapore), Jing Yun Tay (Nanyang Technological University, Singapore), Jason Cheah (Nanyang Technological University, Singapore), and Chee Lip Gan (Nanyang Technological University, Singapore)*

Triple Exploit Chain with Laser Fault Injection on a Secure Element ..... 9
*Olivier Hériveaux (Ledger)*

The More You Know: Improving Laser Fault Injection with Prior Knowledge ..... 18
*Marina Krček (TU Delft), Thomas Ordas (STMicroelectronics), Daniele Fronte (STMicroelectronics), and Stjepan Picek (Radboud University)*

### Fault Attacks to Public Key Cryptosystems

FA-LLLing for RSA: Lattice-Based Fault Attacks against RSA Encryption and Signature ..... 30
*Guillaume Barbu (IDEMIA, France)*

Generalising Fault Attacks to Genus Two Isogeny Cryptosystems ..... 38
*Ariana Goh (DSO National Laboratories, Singapore), Chu-Wee Lim (DSO National Laboratories, Singapore), and Yan Bo Ti (DSO National Laboratories, Singapore)*

### Fault Injection: Techniques, Analysis, Effects

Body Biasing Injection: Impact of Substrate Types on the Induced Disturbances? ..... 50
*Geoffrey Chancel (Université de Montpellier, LIRMM), Jean-Marc Gallière (Université de Montpellier, LIRMM), and Philippe Maurine (Université de Montpellier, LIRMM)*

Quantifying the Speed-Up Offered by Genetic Algorithms during Fault Injection Cartographies ..... 61
*Idris Rais-Ali (Secure-IC S.A.S), Antoine Bouvet (Secure-IC S.A.S), and Sylvain Guilley (Secure-IC S.A.S / Telecom Paris)*

Exploration of Fault Effects on Formal RISC-V Microarchitecture Models ..... 73
*Simon Tollec (Université Paris-Saclay, CEA, France), Mihail Asavoae (Université Paris-Saclay, CEA, France), Damien Couroussé (Université Grenoble Alpes, CEA, France), Karine Heydemann (Sorbonne Université, CNRS, France), and Mathieu Jan (Université Paris-Saclay, CEA, France)*

**Author Index** ..... **85**