

2025 Workshop on Fault Detection and Tolerance in Cryptography (FDTC 2025)

**Kuala Lumpur, Malaysia
14 September 2025**

IEEE Catalog Number:
ISBN:

CFP2586C-POD
979-8-3315-8778-9



Copyright © 2025, IEEE

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:	CFP2586C-POD
ISBN (Print-On-Demand):	979-8-3315-8778-9
ISBN (Online):	979-8-3315-8777-2
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

TABLE OF CONTENTS

AutoPulse – Reproducible Discovery of Electromagnetic Fault Injection Vulnerabilities	1
<i>Marek Wehmer, Maximilian Staab, Jonathan Kramer, Ingmar Baumgart</i>	
Fault Detection in the Control- and Data-Path of Neural Networks	13
<i>Matthias Probst, Manuel Brosch, Augustin Ewald, Michael Gruber, Georg Sigl</i>	
Improving Fault Vulnerability Detection via Rehosting and Comparative Analysis of Open-Source Tools	23
<i>Shoei Nashimoto</i>	
Fault Analysis through Body Bias Injection on the FLASH Memory Accelerator of a Microcontroller	35
<i>Ziling Liao, Florent Bruguier, Philippe Maurine</i>	
From NOP to ADD and Beyond: A Novel Fault-Model Comprising Variable-Length Instruction Sets	46
<i>Khani Marvin Sas, Thomas Martin Johannes Lehrach, Jean-Pierre Seifert</i>	
Fault attacks against UOV-based signatures	52
<i>Sven Bauer, Fabrizio De Santis, Kristjane Koleci</i>	
SIFA on Nonce-based Authenticated Encryption: When Does It Fail? Application to Ascon	61
<i>Viet Sang Nguyen, Vincent Grosso, Pierre-Louis Cayrel</i>	