

2024 Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2024)

**Kobe, Japan
16-18 December 2024**



**IEEE Catalog Number: CFP24F99-POD
ISBN: 979-8-3503-6807-9**

**Copyright © 2024 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:	CFP24F99-POD
ISBN (Print-On-Demand):	979-8-3503-6807-9
ISBN (Online):	979-8-3503-6806-2

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

TABLE OF CONTENTS

AutoGuard: A Secure Implementation of the Conditional Branch Instruction	1
<i>Zeru Lan, Chunlu Wang, Pengfei Qiu, Yu Jin, Yihao Yang, Dongsheng Wang, Gang Qu</i>	
Automated Search of Instructions Vulnerable to Fault Injection Attacks in Command Authorization Checks of a TPM 2.0 Implementation	7
<i>Ville Yli-Mäyry, Thomas Perianin, Sylvain Guilley</i>	
Unveiling Security MRAM-OTP Macro Using MTJ Hard Breakdown Mechanism	13
<i>Jiongze Su, Haoran Du, Quanhai Zhu, Mingtao Chen, Keyang Zhang, Bo Liu, Hao Cai</i>	
Power Side-Channel Key Recovery Attack on a Hardware Implementation of BIKE	19
<i>Luke Beckwith, Huizhen Zhou, Jens-Peter Kaps, Kris Gaj</i>	
A Black-Box Targeted Misclassification Attack on Edge AI with Adversarial Examples Generated from RAW Image Sensor Data	25
<i>Bowen Hu, Weiyang He, Kuo Wang, Chip-Hong Chang</i>	
High Reliable Processor-Based PUF on Voltage Over-Scaling Technique.....	31
<i>Xinyuan Zhao, Yijun Cui, Fei Lyu, Chongyan Gu, Chenghua Wang, Weiqiang Liu</i>	
Exact Template Attacks with Spectral Computation	37
<i>Meriem Mahar, Maamar Ouladj, Sylvain Guilley, Hacène Belbachir, Farid Mokrane</i>	
Sorting Attacks Resilient Authentication Protocol for CMOS Image Sensor Based PUF	43
<i>Anurag Kamal, Vishesh Mishra, Sparsh Mittal, Mahendra Rathor, Chandan Kumar, Urbi Chatterjee</i>	
Analysis and Mitigation of Hybrid CMOS/MRAM DFF Vulnerabilities to Laser Fault Injection	49
<i>Raphaël Comps, Jean-Baptiste Rigaud, Jean-Max Dutertre</i>	
Truly Random Number Generation by Using in-Plane Magnetic Tunnel Junction with Weak Anisotropy	55
<i>You Wang, Chaoyue Zhang, Yefan Xu, Yu Gong, Hao Cai, Weiqiang Liu</i>	
A True Random Number Generator on FPGA with Jitter-Sampling by Ring Generator.....	60
<i>Tuan-Kiet Dang, Trong-Thuc Hoang, Cong-Kha Pham</i>	
Yet Another Physical Leakage Assessment with the Wasserstein Distance.....	66
<i>Haruka Hirata, Yusaku Harada, Yuko Hara, Kazuo Sakiyama, Yang Li</i>	
PreLock: Precision Locking for Protecting Embedded Processor	72
<i>Tomosuke Ichioka, Yohei Watanabe, Yuko Hara</i>	
A Consistency Testing Method for Revealing RISC-V Processor's Undocumented Instructions.....	78
<i>Wen Wang, Peng Liu</i>	
A Novel FPGA Mutually Coupled Configurable Ring Oscillator PUF	84
<i>James Moore, Jack Miskelly, Máire O'Neill, Chongyan Gu</i>	
A Hybrid Simulation Approach for Accurate and Fast System-Level Side-Channel Leakage Evaluation.....	90
<i>Kazuki Monta, Takafumi Oki, Rikuu Hasegawa, Takuya Wadatsumi, Takuji Miki, Makoto Nagata, Lang Lin, Norman Chang</i>	

SecRiSBen: A RISC-V Based SoC Benchmark for Evaluation of Security Verification Tools.....	96
<i>Maoyuan Cai, Aijiao Cui, Yier Jin</i>	

Author Index