2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2022)

Washington, DC, USA
27 – 30 June 2022

IEEE Catalog Number: CFP22HOA-POD
ISBN: 978-1-6654-8533-3

Copyright © 2022 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:	CFP22HOA-POD
ISBN (Print-On-Demand):	978-1-6654-8533-3
ISBN (Online):	978-1-6654-8532-6

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

EnclaveSim:A Micro-Architectural Simulator with Enclave Support 1
Yashika Verma, Dixit Kumar, Biswabandan Panda

Towards Attack Resilient Delay-Based Strong PUFs 5
Nils Wisiol

Security Properties Driven Pre-Silicon Laser Fault Injection Assessment 9
Nitin Pundir, Henian Li, Lang Lin, Norman Chang, Farimah Farahmandi, Mark Tehranipoor

Warm Up Before Circuit De-Obfuscation? An Exploration Through Bounded-Model-Checkers 13
Kimia Zamiri Azar, Hadi Mardani Kamali, Farimah Farahmandi, Mark Tehranipoor

Layout-Level Vulnerability Ranking from Electromagnetic Fault Injection 17
Lang Lin, Jimin Wen, Harsh Shrivastav, Weike Li, Hua Chen, Gang Ni, Sreeja Chowdhury, Calvin Chow, Norman Chang

Structural Analysis Attack on Sequential Circuit Logic Locking 21
Gourav Takhar, Subhajit Roy

A Novel Attack on Machine-Learning Resistant Physical Unclonable Functions 25
Daniel Canaday, Wendson A. S. Barbosa, Andrew Pomerance

System on Chip (SoC) Security Architecture Framework for Isolated Domains Against Threats 29
Siam Haque, Shahnam Mirzaei

Security Threats and Countermeasure Deployment Using Partial Reconfiguration in FPGA CAD Tools 33
Sandeep Sunkavilli, Qiaoyan Yu

Towards an Antivirus for Quantum Computers 37
Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Yongshan Ding, Jakub Szefer

SecSoC: A Secure System on Chip Architecture for IoT Devices 41
Ayman Hroub, Muhammad E. S. Elrabaa

Characterizing Side-Channel Leakage of DNN Classifiers Though Performance Counters 45
Saikat Majumdar, Mohammad Hossein Samavatian, Radu Teodorescu

Detecting Continuous Jamming Attack Using Ultra-Low Power RSSI Circuit 49
Ankit Mittal, Aatmesh Shrivastava

Secuirty Metrics for Logic Circuits 53
Ruben Purdy, Danielle Duvalsaint, R. D. Shawn Blanton

SpecPref: High Performing Speculative Attacks Resilient Hardware Prefetchers 57
Tarun Solanki, Biswabandan Panda

pHGen: A pH-Based Key Generation Mechanism Using ISFETs 61
Elmira Moussavi, Dominik Sisejkovic, Fabian Brings, Daniyar Kizatov, Animesh Singh, Xuan Thang Vu, Rainer Leupers, Sven Ingebrandt, Vivek Pachauri, Farhad Merchant

Safeguarding Unmanned Aerial Vehicles Against Side Channel Analysis Via Motor Noise Injection 65
Timothy Radtke, Cristinel Ababei

WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography 69
Markku-Juhani O. Saarinen

Chosen-Plaintext Attack on Energy-Efficient Hardware Implementation of GIFT-COFB 73
Yadi Zhong, Ujjwal Guin

Error Correction Attacks on BACnet MS/TP 77
Tsion Yimer, Edmund Smith, Paige Harvey, Marcial Tienteu, Kevin Kornegay

Insertion of Random Delay with Context-Aware Dummy Instructions Generator in a RISC-V Processor 81
Gaëtan Leplus, Olivier Savry, Lilian Bossuet

Contact PUF: Highly Stable Physical Unclonable Functions Based on Contact Failure Probability in 180 nm, 130 nm, and 28 nm CMOS Processes 85
Duhyun Jeon, Dongmin Lee, Dong Kyue Kim, Byong-Deok Choi

Efficient Targeted Bit-Flip Attack Against the Local Binary Pattern Network 89
Arman Roohi, Shaahin Angizi

Efficient and Side-Channel Resistant Design of High-Security Ed448 on ARM Cortex-M4 93
Mila Anastasova, Mojtaba Bisheh-Niasar, Hwajeong Seo, Reza Azarderakhsh, Mehran Mozaffari Kermani

Detecting Laser Fault Injection Attacks Via Time-to-Digital Converter Sensors 97
Mohammad Ebrahimabadi, Suhee Sanjana Mehjabin, Raphael Viera, Sylvain Guilley, Jean-Luc Danger, Jean-Max Dutertre, Naghmeh Karimi

True Random Number Generation with the Shift-Register Reconvergent-Fanout (SiRF) PUF 101
Nafis Irtija, Eirini Eleni Tsiropoulou, Cyrus Minwalla, Jim Plusquellic

Dynamic Key Updates for LUT Locked Design 105
Jakub Slowik, Gregory Williams, Rummah Albashir, Anthony Samagio, Geraldine Shirley Nicholas, Fareena Saqib

PCB Component Detection for Hardware Assurance: A Feature Selection-Based Approach 109
Shajib Ghosh, Mohammad Tahsin Mostafiz, Suprith Reddy Gurudu, Shayan Taheri, Navid Asadizanjani

Metrics for Assessing Security of System-on-Chip 113
Sujan Kumar Saha, Joel Mandebi Mbongue, Christophe Bobda

FTC: A Universal Sensor for Fault Injection Attack Detection 117
M. Rafid Muttaki, Tao Zhang, Mark Tehranipoor, Farimah Farahmandi

Hardware Trojan Detection at LUT: Where Structural Features Meet Behavioral Characteristics 121
Lingjuan Wu, Xuelin Zhang, Siyi Wang, Wei Hu

Security Analysis of Delay-Based Strong PUFs with Multiple Delay Lines 125
Anita Aghaie, Amir Moradi, Johannes Tobisch, Nils Wisiol

Mathematical Model of Strong Physically Unclonable Functions Based on Hybrid Boolean Networks 129
Noeloikeau Charlot, Daniel J. Gauthier, Daniel Canaday, Andrew Pomerance

On the Feasibility of Training-Time Trojan Attacks Through Hardware-Based Faults in Memory 133
Kunbei Cai, Zhenkai Zhang, Fan Yao

Identification and Classification of Corrupted PUF Responses Via Machine Learning 137
Reshmi Suragani, Emiliia Nazarenko, Nikolaos Athanasios Anagnostopoulos, Nico Mexis, Elif Bilge Kavun

Hardening Hardware Accelerartor Based CNN Inference Phase Against Adversarial Noises 141
Tolulope A. Odetola, Adewale Adeyemo, Syed Rafay Hasan

Global Attack and Remedy on IC-Specific Logic Encryption 145
Amin Rezaei, Ava Hedayatipour, Hossein Sayadi, Mehrdad Aliasgari, Hai Zhou

Evaluating the Impact of Hardware Faults on Program Execution in a Microkernel Environment 149
Yohannes B. Bekele, Daniel B. Limbrick

Practical Performance of Analog Attack Techniques 153
Vaibhav Venugopal Rao, Kyle Juretus, Ioannis Savidis

Systolic Acceleration of Polynomial Multiplication for KEM Saber and Binary Ring-LWE Post-Quantum Cryptography 157
Tianyou Bao, Pengzhou He, Jiafeng Xie

A Lightweight Mutual Authentication Protocol Based on Physical Unclonable Functions 161
Saeed Abdolinezhad, Axel Sikora

Oblivious Intrusion Detection System 165
Mahmoud Abdelhafeez Sayed, Mostafa Taha

A Modeling Attack on the Sub-Threshold Current Array PUF 169
Yun Liu, Yongliang Chen, Xiaole Cui

Partial Reconfiguration for Run-Time Memory Faults and Hardware Trojan Attacks Detection 173
Ying Li, Lan Chen, Jian Wang, Guanfei Gong

Securing Hardware Accelerator During High-Level Synthesis 177
Dipanjan Roy, Sabiya Jani Shaik, Sonam Sharma

PUF-Based Secure Test Wrapper Design for Network-On-Chip 181
Ying Zhang, Yuanxiang Li, Xin Chen, Jizhong Yang, Yifeng Hua, Jiaoyan Yao

Author Index