

Domenic Forte

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/3733721/publications.pdf>

Version: 2024-02-01

81
papers

2,223
citations

361413

20
h-index

315739

38
g-index

81
all docs

81
docs citations

81
times ranked

1249
citing authors

#	ARTICLE	IF	CITATIONS
1	Benchmarking of Hardware Trojans and Maliciously Affected Circuits. Journal of Hardware and Systems Security, 2017, 1, 85-102.	1.3	191
2	A Survey on Chip to System Reverse Engineering. ACM Journal on Emerging Technologies in Computing Systems, 2017, 13, 1-34.	2.3	162
3	On Reverse Engineering-Based Hardware Trojan Detection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, 35, 49-57.	2.7	114
4	On application of one-class SVM to reverse engineering-based hardware Trojan detection. , 2014, , .		97
5	Memristor PUF—A Security Primitive: Theory and Experiment. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2015, 5, 222-229.	3.6	94
6	Counterfeit Integrated Circuits. , 2015, , .		79
7	A Novel Built-In Self-Authentication Technique to Prevent Inserting Hardware Trojans. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33, 1778-1791.	2.7	70
8	Highly Reliable Key Generation From Electrocardiogram (ECG). IEEE Transactions on Biomedical Engineering, 2017, 64, 1400-1411.	4.2	66
9	Probing Attacks on Integrated Circuits: Challenges and Research Opportunities. IEEE Design and Test, 2017, 34, 63-71.	1.2	65
10	An Aging-Resistant RO-PUF for Reliable Key Generation. IEEE Transactions on Emerging Topics in Computing, 2015, , 1-1.	4.6	64
11	Anti-counterfeit Techniques: From Design to Resign. , 2013, , .		62
12	Temperature Tracking: Toward Robust Run-Time Detection of Hardware Trojans. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1577-1585.	2.7	61
13	Low-cost On-Chip Structures for Combating Die and IC Recycling. , 2014, , .		60
14	Aging analysis for recycled FPGA detection. , 2014, , .		59
15	Efficient and secure split manufacturing via obfuscated built-in self-authentication. , 2015, , .		59
16	FORTIS. ACM Transactions on Design Automation of Electronic Systems, 2016, 21, 1-20.	2.6	52
17	Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives. ACM Journal on Emerging Technologies in Computing Systems, 2021, 17, 1-53.	2.3	44
18	Non-fiducial PPG-based authentication for healthcare application. , 2017, , .		43

#	ARTICLE	IF	CITATIONS
19	Development and Evaluation of Hardware Obfuscation Benchmarks. Journal of Hardware and Systems Security, 2018, 2, 142-161.	1.3	38
20	Security-Aware FSM Design Flow for Identifying and Mitigating Vulnerabilities to Fault Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 1003-1016.	2.7	38
21	Obfuscation-Based Protection Framework against Printed Circuit Boards Unauthorized Operation and Reverse Engineering. ACM Transactions on Design Automation of Electronic Systems, 2017, 22, 1-31.	2.6	31
22	Hardware trojan detection through information flow security verification. , 2017, , .		31
23	PCB Reverse Engineering Using Nondestructive X-ray Tomography and Advanced Image Processing. IEEE Transactions on Components, Packaging and Manufacturing Technology, 2017, , 1-8.	2.5	30
24	Security vulnerability analysis of design-for-test exploits for asset protection in SoCs. , 2017, , .		29
25	Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT. IEEE Access, 2019, 7, 49135-49149.	4.2	29
26	Chip-level anti-reverse engineering using transformable interconnects. , 2015, , .		25
27	Recycled FPGA Detection Using Exhaustive LUT Path Delay Characterization and Voltage Scaling. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2897-2910.	3.1	25
28	PUFmeter a Property Testing Tool for Assessing the Robustness of Physically Unclonable Functions to Machine Learning Attacks. IEEE Access, 2019, 7, 122513-122521.	4.2	25
29	Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 86-118.	0.0	25
30	ECG Biometric: Spoofing and Countermeasures. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2020, 2, 257-270.	4.4	22
31	Systematic Correlation and Cell Neighborhood Analysis of SRAM PUF for Robust and Unique Key Generation. Journal of Hardware and Systems Security, 2017, 1, 137-155.	1.3	21
32	Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security. Journal of Hardware and Systems Security, 2018, 2, 15-32.	1.3	20
33	A layout-driven framework to assess vulnerability of ICs to microprobing attacks. , 2016, , .		19
34	Security Beyond CMOS: Fundamentals, Applications, and Roadmap. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3420-3433.	3.1	19
35	Probing Assessment Framework and Evaluation of Antiprobing Solutions. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 1239-1252.	3.1	19
36	Genetic Algorithm for hardware Trojan detection with ring oscillator network (RON). , 2015, , .		18

#	ARTICLE	IF	CITATIONS
37	Recycled FPGA detection using exhaustive LUT path delay characterization. , 2016, , .		18
38	On the vulnerability of ECG verification to online presentation attacks. , 2017, , .		18
39	A Physical Design Flow Against Front-Side Probing Attacks by Internal Shielding. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 2152-2165.	2.7	18
40	Impact of X-Ray Tomography on the Reliability of Integrated Circuits. IEEE Transactions on Device and Materials Reliability, 2017, 17, 59-68.	2.0	17
41	SCARe: An SRAM-Based Countermeasure Against IC Recycling. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2018, 26, 744-755.	3.1	15
42	Power-based side-channel instruction-level disassembler. , 2018, , .		15
43	EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2020, 28, 363-375.	3.1	15
44	PreLatPUF: Exploiting DRAM Latency Variations for Generating Robust Device Signatures. IEEE Access, 2019, 7, 81106-81120.	4.2	13
45	A Metal-Via Resistance Based Physically Unclonable Function with 1.18% Native Instability. , 2019, , .		12
46	Detecting Dye-Contaminated Vegetables Using Low-Field NMR Relaxometry. Foods, 2021, 10, 2232.	4.3	12
47	Reliability vs. security: Challenges and opportunities for developing reliable and secure integrated circuits. , 2016, , .		11
48	SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware. IEEE Transactions on Dependable and Secure Computing, 2016, , 1-1.	5.4	11
49	Leveraging Side-Channel Information for Disassembly and Security. ACM Journal on Emerging Technologies in Computing Systems, 2020, 16, 1-21.	2.3	11
50	Automated Defective Pin Detection for Recycled Microelectronics Identification. Journal of Hardware and Systems Security, 2019, 3, 250-260.	1.3	10
51	A stochastic approach to analog physical unclonable function. , 2016, , .		9
52	REFICS: Assimilating Data-Driven Paradigms Into Reverse Engineering and Hardware Assurance on Integrated Circuits. IEEE Access, 2021, 9, 131955-131976.	4.2	9
53	Enhancing noise sensitivity of embedded SRAMs for robust true random number generation in SoCs. , 2016, , .		8
54	Obfuscated Built-In Self-Authentication With Secure and Efficient Wire-Lifting. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 1981-1994.	2.7	8

#	ARTICLE	IF	CITATIONS
55	Performance optimization for on-chip sensors to detect recycled ICs. , 2015, , .		7
56	EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection with Demonstration on Remarked and Cloned ICs. , 2018, , .		7
57	Rockâ€™nâ€™roll PUFs: crafting provably secure pufs from less secure ones (extended version). Journal of Cryptographic Engineering, 2021, 11, 105-118.	1.8	7
58	PATRON: A Pragmatic Approach for Encoding Laser Fault Injection Resistant FSMs. , 2021, , .		7
59	Automated Detection and Localization of Counterfeit Chip Defects by Texture Analysis in Infrared (IR) Domain. , 2020, , .		7
60	Obfuscated Built-In Self-authentication. , 2017, , 263-289.		6
61	A stochastic all-digital weak physically unclonable function for analog/mixed-signal applications. , 2017, , .		5
62	Recycled SoC Detection Using LDO Degradation. SN Computer Science, 2020, 1, 1.	3.6	5
63	A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks. , 2018, , .		4
64	Automated Detection of Pin Defects on Counterfeit Microelectronics. , 2018, , .		4
65	Self-timed Sensors for Detecting Static Optical Side Channel Attacks. , 2022, , .		4
66	Poly-Si-Based Physical Unclonable Functions. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3207-3217.	3.1	3
67	Bimodal Oscillation as a Mechanism for Autonomous Majority Voting in PUFs. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2018, 26, 2431-2442.	3.1	3
68	First Auto-Magnifier Platform for Hardware Assurance and Reverse Engineering Integrated Circuits. Microscopy and Microanalysis, 2019, 25, 226-227.	0.4	3
69	Improving the Quality of Delay-Based PUFs via Optical Proximity Correction. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32, 1879-1891.	2.7	2
70	Aging attacks for key extraction on permutation-based obfuscation. , 2016, , .		2
71	Selective Enhancement of Randomness at the Materials Level: Poly-Si Based Physical Unclonable Functions (PUFs). , 2016, , .		2
72	Resistance Drift and Crystallization in Suspended and On-oxide Phase Change Memory Line Cells. , 2019, , .		2

#	ARTICLE	IF	CITATIONS
73	A Metal-Via Resistance Based Physically Unclonable Function With Backend Incremental ADC. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68, 4700-4709.	5.4	2
74	An Analysis of Enrollment and Query Attacks on Hierarchical Bloom Filter-Based Biometric Systems. IEEE Transactions on Information Forensics and Security, 2021, 16, 5294-5309.	6.9	2
75	Aging resilient RO PUF with increased reliability in FPGA. , 2017, , .		1
76	Hierarchical Bloom Filter Framework for Security, Space-efficiency, and Rapid Query Handling in Biometric Systems. , 2019, , .		1
77	Permutation Network De-obfuscation. ACM Journal on Emerging Technologies in Computing Systems, 2020, 16, 1-25.	2.3	1
78	Harnessing Nanoscale Device Properties for Hardware Security. , 2015, , .		0
79	Guest Editorial: Hardware Reverse Engineering and Obfuscation. Journal of Hardware and Systems Security, 2018, 2, 287-288.	1.3	0
80	BLOcKeR: A Biometric Locking Paradigm for IoT and the Connected Person. Journal of Hardware and Systems Security, 2021, 5, 223.	1.3	0
81	Joint Optimization of NCL PUF Using Frequency-based Analysis and Evolutionary Algorithm. , 2022, , .		0