Ramesh Karri

List of Publications by Year
in descending order

263 papers	7,900 citations	117625 34 h-index	98798 67 g-index
271 all docs	271 docs citations	271 times ranked	3226 citing authors

#	Article	IF	Citations
1	Fuzzing+Hardware Performance Counters-Based Detection of Algorithm Subversion Attacks on Postquantum Signature Schemes. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42, 384-396.	2.7	3
2	Learning Malicious Circuits in FPGA Bitstreams. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42, 726-739.	2.7	4
3	Opening the Doors to Dynamic Camouflaging: Harnessing the Power of Polymorphic Devices. IEEE Transactions on Emerging Topics in Computing, 2022, 10, 137-156.	4.6	15
4	Towards a New Thermal Monitoring Based Framework for Embedded CPS Device Security. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 524-536.	5.4	15
5	Runtime Malware Detection Using Embedded Trace Buffers. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41, 35-48.	2.7	2
6	Robust Deep Learning for IC Test Problems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41, 183-195.	2.7	9
7	Cyber Insurance Against Cyberattacks on Electric Vehicle Charging Stations. IEEE Transactions on Smart Grid, 2022, 13, 1529-1541.	9.0	14
8	Trojan Detection in Embedded Systems With FinFET Technology. IEEE Transactions on Computers, 2022, 71, 3061-3071.	3.4	4
9	HPC-Based Malware Detectors Actually Work: Transition to Practice After a Decade of Research. IEEE Design and Test, 2022, 39, 23-32.	1.2	1
10	Protecting Hardware IP Cores During High-Level Synthesis. , 2022, , 95-115.		0
11	HOLL: Program Synthesis for Higher Order Logic Locking. Lecture Notes in Computer Science, 2022, , 3-24.	1.3	9
12	Obfuscation for IP Protection. , 2022, , 87-109.		0
13	Watermarking for IP Protection. , 2022, , 61-85.		0
14	Detecting Hardware Trojans in PCBs Using Side Channel Loopbacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2022, 30, 926-937.	3.1	9
15	A Composable Design Space Exploration Framework to Optimize Behavioral Locking. , 2022, , .		5
16	FLAW3D: A Trojan-Based Cyber Attack on the Physical Outcomes of Additive Manufacturing. IEEE/ASME Transactions on Mechatronics, 2022, 27, 5361-5370.	5.8	13
17	False data injection attacks on data markets for electric vehicle charging stations. Advances in Applied Energy, 2022, 7, 100098.	13.2	3
18	How Secure Are Checkpoint-Based Defenses in Digital Microfluidic Biochips?. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 143-156.	2.7	8

#	Article	IF	Citations
19	Training Data Poisoning in ML-CAD: Backdooring DL-Based Lithographic Hotspot Detectors. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1244-1257.	2.7	1
20	Toward Hardware-Based IP Vulnerability Detection and Post-Deployment Patching in Systems-on-Chip. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1158-1171.	2.7	8
21	A Survey of Cybersecurity of Digital Manufacturing. Proceedings of the IEEE, 2021, 109, 495-516.	21.3	22
22	Security Against Data-Sniffing and Alteration Attacks in IJTAG. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1301-1314.	2.7	5
23	HOST: HLS Obfuscations against SMT ATtack. , 2021, , .		5
24	Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society, 2021, 66, 102682.	10.4	19
25	Special Session: Machine Learning for Semiconductor Test and Reliability. , 2021, , .		6
26	Causative Cyberattacks on Online Learning-Based Automated Demand Response Systems. IEEE Transactions on Smart Grid, 2021, 12, 3548-3559.	9.0	8
27	Efficient Hardware Implementation of PQC Primitives and PQC algorithms Using High-Level Synthesis. , 2021, , .		7
28	ASSURE: RTL Locking Against an Untrusted Foundry. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2021, 29, 1306-1318.	3.1	35
29	Hardware Performance Counters: Ready-Made vs Tailor-Made. Transactions on Embedded Computing Systems, 2021, 20, 1-26.	2.9	1
30	Uncertainty quantification in dimensions dataset of additive manufactured NIST standard test artifact. Data in Brief, 2021, 38, 107286.	1.0	3
31	Bias Busters: Robustifying DL-Based Lithographic Hotspot Detectors Against Backdooring Attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 2077-2089.	2.7	2
32	Attacking a CNN-based Layout Hotspot Detector Using Group Gradient Method. , 2021, , .		7
33	Thwarting Bio-IP Theft Through Dummy-Valve-Based Obfuscation. IEEE Transactions on Information Forensics and Security, 2021, 16, 2076-2089.	6.9	8
34	Protection against Counterfeiting Attacks in 3D Printing by Streaming Signature-embedded Manufacturing Process Instructions. , 2021, , .		4
35	Invited: Independent Verification and Validation of Security-Aware EDA Tools and IP. , 2021, , .		0
36	Fortifying RTL Locking Against Oracle-Less (Untrusted Foundry) and Oracle-Guided Attacks. , 2021, , .		15

#	Article	IF	Citations
37	Microfluidic Device Security. , 2021, , 555-577.		0
38	Security Closure of Physical Layouts ICCAD Special Session Paper. , 2021, , .		3
39	Exploring eFPGA-based Redaction for IP Protection. , 2021, , .		17
40	Synthesis of Tamper-Resistant Pin-Constrained Digital Microfluidic Biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 171-184.	2.7	6
41	Analysis and Design of Tamper-Mitigating Microfluidic Routing Fabrics. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 1003-1016.	2.7	3
42	Toward Increasing the Difficulty of Reverse Engineering of RSFQ Circuits. IEEE Transactions on Applied Superconductivity, 2020, 30, 1-13.	1.7	14
43	Anomaly Detection in Real-Time Multi-Threaded Processes Using Hardware Performance Counters. IEEE Transactions on Information Forensics and Security, 2020, 15, 666-680.	6.9	44
44	Detection: Randomizing Checkpoints on Cyberphysical Digital Microfluidic Biochips. , 2020, , 79-107.		0
45	A Theoretical Study of Hardware Performance Counters-Based Malware Detection. IEEE Transactions on Information Forensics and Security, 2020, 15, 512-525.	6.9	40
46	Bio-chemical Assay Locking to Thwart Bio-IP Theft. ACM Transactions on Design Automation of Electronic Systems, 2020, 25, 1-20.	2.6	6
47	Poisoning the (Data) Well in ML-Based CAD: A Case Study of Hiding Lithographic Hotspots. , 2020, , .		14
48	Exposing Hardware Trojans in Embedded Platforms via Short-Term Aging. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 3519-3530.	2.7	9
49	Anomaly Detection in Embedded Systems Using Power and Memory Side Channels. , 2020, , .		4
50	Cybersecurity Road Map for Digital Manufacturing. Computer, 2020, 53, 80-84.	1.1	2
51	Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. IEEE Access, 2020, 8, 214434-214453.	4.2	84
52	Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. IEEE Access, 2020, 8, 47322-47333.	4.2	68
53	COPPTCHA: COPPA Tracking by Checking Hardware-Level Activity. IEEE Transactions on Information Forensics and Security, 2020, 15, 3213-3226.	6.9	8
54	Is Register Transfer Level Locking Secure?. , 2020, , .		17

#	Article	IF	Citations
55	Programmable Daisychaining of Microelectrodes to Secure Bioassay IP in MEDA Biochips. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2020, 28, 1269-1282.	3.1	8
56	Hardware Trojan Detection Using Controlled Circuit Aging. IEEE Access, 2020, 8, 77415-77434.	4.2	19
57	Toward Secure Checkpointing for Micro-Electrode-Dot-Array Biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 4908-4920.	2.7	5
58	Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?. IEEE Transactions on Smart Grid, 2020, 11, 5099-5113.	9.0	72
59	Secure Assay Execution on MEDA Biochips to Thwart Attacks Using Real-Time Sensing. ACM Transactions on Design Automation of Electronic Systems, 2020, 25, 1-25.	2.6	7
60	Adversarial Perturbation Attacks on ML-based CAD. ACM Transactions on Design Automation of Electronic Systems, 2020, 25, 1-31.	2.6	16
61	Prevention: Tamper-Resistant Pin-Constrained Digital Microfluidic Biochips. , 2020, , 51-77.		0
62	Security and Trust. , 2020, , 19-49.		0
63	Molecular Barcoding as a Defense Against Benchtop Biochemical Attacks on DNA Fingerprinting and Information Forensics. IEEE Transactions on Information Forensics and Security, 2020, 15, 3595-3609.	6.9	7
64	Toward Secure and Trustworthy Cyberphysical Microfluidic Biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 589-603.	2.7	23
65	TaintHLS: High-Level Synthesis for Dynamic Information Flow Tracking. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 798-808.	2.7	26
66	Security Assessment of Micro-Electrode-Dot-Array Biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 1831-1843.	2.7	12
67	Toward Secure Microfluidic Fully Programmable Valve Array Biochips. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2755-2766.	3.1	12
68	Hardware Trojans Inspired IP Watermarks. IEEE Design and Test, 2019, 36, 72-79.	1.2	11
69	Desieve the Attacker: Thwarting IP Theft in Sieve-Valve-based Biochips. , 2019, , .		9
70	PREEMPT. , 2019, , .		16
71	Can Multi-Layer Microfluidic Design Methods Aid Bio-Intellectual Property Protection?. , 2019, , .		2
72	Locking the Design of Building Blocks for Quantum Circuits. Transactions on Embedded Computing Systems, 2019, 18, 1-15.	2.9	4

#	Article	IF	Citations
73	High-Level Synthesis of Benevolent Trojans. , 2019, , .		7
74	Security Assessment of Microfluidic Fully-Programmable-Valve-Array Biochips. , 2019, , .		7
75	Reversible Circuits: IC/IP Piracy Attacks and Countermeasures. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 2523-2535.	3.1	3
76	Execution of provably secure assays on MEDA biochips to thwart attacks. , 2019, , .		17
77	Multi-Tenant FPGA-based Reconfigurable Systems: Attacks and Defenses. , 2019, , .		16
78	Identification of Synthesis Approaches for IP/IC Piracy of Reversible Circuits. ACM Journal on Emerging Technologies in Computing Systems, 2019, 15, 1-17.	2.3	4
79	Security Assessment of Microfluidic Immunoassays. , 2019, , .		3
80	CAD-Base. ACM Transactions on Design Automation of Electronic Systems, 2019, 24, 1-30.	2.6	31
81	Bio-Protocol Watermarking on Digital Microfluidic Biochips. IEEE Transactions on Information Forensics and Security, 2019, 14, 2901-2915.	6.9	23
82	Split Manufacturing-Based Register Transfer-Level Obfuscation. ACM Journal on Emerging Technologies in Computing Systems, 2019, 15, 1-22.	2.3	3
83	IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Past, Present, and Future. , 2019, , .		2
84	Can Monitoring System State + Counting Custom Instruction Sequences Aid Malware Detection?. , 2019, , .		2
85	Power, Area, Speed, and Security (PASS) Trade-Offs of NIST PQC Signature Candidates Using a C to ASIC Design Flow. , 2019, , .		6
86	Stealthy Rootkits in Smart Grid Controllers. , 2019, , .		7
87	Programmable Daisychaining of Microelectrodes for IP Protection in MEDA Biochips. , 2019, , .		4
88	Black-Hat High-Level Synthesis: Myth or Reality?. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 913-926.	3.1	13
89	On the Difficulty of Inserting Trojans in Reversible Computing Architectures. IEEE Transactions on Emerging Topics in Computing, 2018, , 1-1.	4.6	6
90	Securing Hardware Accelerators: A New Challenge for High-Level Synthesis. IEEE Embedded Systems Letters, 2018, 10, 77-80.	1.9	63

#	Article	IF	Citations
91	Secure Randomized Checkpointing for Digital Microfluidic Biochips. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 1119-1132.	2.7	42
92	DPFEE: A High Performance Scalable Pre-Processor for Network Security Systems. IEEE Transactions on Multi-Scale Computing Systems, 2018, 4, 55-68.	2.4	9
93	Tamper-resistant pin-constrained digital microfluidic biochips. , 2018, , .		6
94	Abetting Planned Obsolescence by Aging 3D Networks-on-Chip. , 2018, , .		6
95	Shadow attacks on MEDA biochips. , 2018, , .		7
96	IC/IP piracy assessment of reversible logic. , 2018, , .		4
97	TAO: Techniques for Algorithm-Level Obfuscation during High-Level Synthesis. , 2018, , .		11
98	Hardware Trojan Detection Using the Order of Path Delay. ACM Journal on Emerging Technologies in Computing Systems, 2018, 14, 1-23.	2.3	20
99	TAO. , 2018, , .		31
100	Locking of biochemical assays for digital microfluidic biochips. , 2018, , .		25
101	Hardware Trojan detection using path delay order encoding with process variation tolerance. , 2018, , .		3
102	Process-Aware Covert Channels Using Physical Instrumentation in Cyber-Physical Systems. IEEE Transactions on Information Forensics and Security, 2018, 13, 2761-2771.	6.9	27
103	Securing IJTAG against data-integrity attacks. , 2018, , .		10
104	Secure and Flexible Trace-Based Debugging of Systems-on-Chip. ACM Transactions on Design Automation of Electronic Systems, 2017, 22, 1-25.	2.6	7
105	Automotive Electrical and Electronic Architecture Security via Distributed In-Vehicle Traffic Monitoring. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 36, 1790-1803.	2.7	44
106	Research Challenges in Security-Aware Physical Design. , 2017, , .		0
107	Guest Editorsâ€™ Introduction: Cyber-Physical Systems Security and Privacy. IEEE Design and Test, 2017, 34, 5-6.	1.2	2
108	Boolean Circuit Camouflage. , 2017, , .		5

#	Article	IF	Citations
109	Security Implications of Cyberphysical Flow-Based Microfluidic Biochips. , 2017, , .		20
110	TAINT: Tool for Automated INsertion of Trojans. , 2017, , .		8
111	Security Trade-Offs in Microfluidic Routing Fabrics. , 2017, , .		14
112	Fingerprinting Field Programmable Gate Arrays. , 2017, , .		9
113	Identifying Reversible Circuit Synthesis Approaches to Enable IP Piracy Attacks. , 2017, , .		3
114	Process-aware side channel monitoring for embedded control system security. , 2017, , .		6
115	Emerging (un-)reliability based security threats and mitigations for embedded systems. , 2017, , .		17
116	Hybrid silicon CMOS-carbon nanotube physically unclonable functions. , 2017, , .		0
117	Optimal checkpointing for secure intermittently-powered IoT devices. , 2017, , .		18
118	Physical Unclonable Functions and Intellectual Property Protection Techniques. , 2017, , 199-222.		2
119	FPGA Trust Zone: Incorporating trust and reliability into FPGA designs. , 2016, , .		13
120	Microfluidic encryption of on-chip biochemical assays. , 2016, , .		37
121	Can flexible, domain specific programmable logic prevent IP theft?. , 2016, , .		1
122	Securing pressure measurements using SensorPUFs. , 2016, , .		8
123	Securing digital microfluidic biochips by randomizing checkpoints. , 2016, , .		17
124	Building Trustworthy Systems Using Untrusted Components: A High-Level Synthesis Approach. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016, 24, 2946-2959.	3.1	60
125	Formal Security Verification of Third Party Intellectual Property Cores for Information Leakage. , 2016, , .		40
126	The Cybersecurity Landscape in Industrial Control Systems. Proceedings of the IEEE, 2016, 104, 1039-1057.	21.3	249

#	Article	IF	Citations
127	Hardware Performance Counter-Based Malware Identification and Detection with Adaptive Compressive Sensing. Transactions on Architecture and Code Optimization, 2016, 13, 1-23.	2.0	39
128	Manufacturing and Security Challenges in 3D Printing. Jom, 2016, 68, 1872-1881.	1.9	172
129	Cybersecurity for Control Systems: A Process-Aware Perspective. IEEE Design and Test, 2016, 33, 75-83.	1.2	72
130	Controlling your control flow graph. , 2016, , .		6
131	Malicious Firmware Detection with Hardware Performance Counters. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 160-173.	2.4	40
132	BRAIN: BehavioR Based Adaptive Intrusion Detection in Networks: Using Hardware Performance Counters to Detect DDoS Attacks. , 2016, , .		38
133	Can Algorithm Diversity in Stream Cipher Implementation Thwart (Natural and) Malicious Faults?. IEEE Transactions on Emerging Topics in Computing, 2016, 4, 363-373.	4.6	1
134	Security Assessment of Cyberphysical Digital Microfluidic Biochips. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2016, 13, 445-458.	3.0	50
135	On Improving the Security of Logic Locking. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, 35, 1411-1424.	2.7	232
136	Fault Attacks on AES and Their Countermeasures. , 2016, , 163-208.		18
137	Reusing Hardware Performance Counters to Detect and Identify Kernel Control-Flow Modifying Rootkits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, 35, 485-498.	2.7	57
138	Exploiting Small Leakages in Masks to Turn a Second-Order Attack into a First-Order Attack and Improved Rotating Substitution Box Masking with Linear Code Cosets. Scientific World Journal, The, 2015, 2015, 1-10.	2.1	7
139	A secure design-for-test infrastructure for lifetime security of SoCs. , 2015, , .		2
140	Secure design-for-debug for Systems-on-Chip. , 2015, , .		8
141	Belling the CAD: Toward Security-Centric Electronic System Design. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1756-1769.	2.7	25
142	Deep Packet Field Extraction Engine (DPFEE): A pre-processor for network intrusion detection and denial-of-service detection systems. , 2015, , .		6
143	Exploiting small leakages in masks to turn a second-order attack into a first-order attack. , 2015, , .		2
144	ConFirm: Detecting firmware modifications in embedded systems using Hardware Performance Counters. , 2015, , .		55

#	Article	IF	Citations
145	Security implications of cyberphysical digital microfluidic biochips. , 2015, , .		23
146	Fault Analysis-Based Logic Encryption. IEEE Transactions on Computers, 2015, 64, 410-424.	3.4	352
147	Security Vulnerabilities of Emerging Nonvolatile Main Memories and Countermeasures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 2-15.	2.7	35
148	Guest Editorial Special Section on Hardware Security and Trust. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 873-874.	2.7	3
149	Nano Meets Security: Exploring Nanoelectronic Devices for Security Applications. Proceedings of the IEEE, 2015, 103, 829-849.	21.3	102
150	Novel Test-Mode-Only Scan Attack and Countermeasure for Compression-Based Scan Architectures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 808-821.	2.7	43
151	Modeling, Detection, and Diagnosis of Faults in Multilevel Memristor Memories. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 822-834.	2.7	61
152	Reliable Integrity Checking in Multicore Processors. Transactions on Architecture and Code Optimization, 2015, 12, 1-23.	2.0	3
153	Simulation and analysis of negative-bias temperature instability aging on power analysis attacks. , 2015, , .		3
154	Detecting malicious modifications of data in third-party intellectual property cores. , 2015, , .		80
155	On enhancing the debug architecture of a system-on-chip (SoC) to detect software attacks. , 2015, , .		9
156	Security analysis of concurrent error detection against differential fault analysis. Journal of Cryptographic Engineering, 2015, 5, 153-169.	1.8	61
157	Improving Tolerance to Variations in Memristor-Based Applications Using Parallel Memristors. IEEE Transactions on Computers, 2015, 64, 733-746.	3.4	34
158	New Scan-Based Attack Using Only the Test Mode and an Input Corruption Countermeasure. IFIP Advances in Information and Communication Technology, 2015, , 48-68.	0.7	2
159	Test-mode-only scan attack and countermeasure for contemporary scan architectures. , 2014, , .		19
160	AES design space exploration new line for scan attack resiliency. , 2014, , .		7
161	Shielding Heterogeneous MPSoCs From Untrustworthy 3PIPs Through Security- Driven Task Scheduling. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 461-472.	4.6	41
162	Shielding and securing integrated circuits with sensors. , 2014, , .		30

#	Article	IF	Citations
163	Low-Cost Concurrent Error Detection for GCM and CCM. Journal of Electronic Testing: Theory and Applications (JETTA), 2014, 30, 725.	1.2	4
164	Can the SHIELD protect our integrated circuits?. , 2014, , .		9
165	Reusing the IEEE 1500 design for test infrastructure for security monitoring of Systems-on-Chip. , 2014, , .		5
166	A Primer on Hardware Security: Models, Methods, and Metrics. Proceedings of the IEEE, 2014, 102, 1283-1295.	21.3	471
167	Detection, diagnosis, and repair of faults in memristor-based memories. , 2014, , .		24
168	NREPO: Normal basis Recomputing with Permuted Operands. , 2014, , .		7
169	Test-mode-only scan attack using the boundary scan chain. , 2014, , .		20
170	Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors. , 2014, , .		27
171	New scan attacks against state-of-the-art countermeasures and DFT. , 2014, , .		15
172	Regaining Trust in VLSI Design: Design-for-Trust Techniques. Proceedings of the IEEE, 2014, 102, 1266-1282.	21.3	68
173	Approximating the age of RF/analog circuits through re-characterization and statistical estimation. , 2014, , .		0
174	Trustworthy Hardware [Scanning the Issue]. Proceedings of the IEEE, 2014, 102, 1123-1125.	21.3	4
175	Special Issue on Emerging Nanoscale Architectures for Hardware Security, Trust, and Reliability: Part 1. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 2-3.	4.6	5
176	Detecting Kernel Control-Flow Modifying Rootkits. Advances in Information Security, 2014, , 177-187.	1.2	4
177	Securing Processors Against Insider Attacks: A Circuit-Microarchitecture Co-Design Approach. IEEE Design and Test, 2013, 30, 35-44.	1.2	24
178	Run-time detection of hardware Trojans: The processor protection unit. , 2013, , .		30
179	NumChecker. , 2013, , .		77
180	Hardware security strategies exploiting nanoelectronic circuits. , 2013, , .		28

#	Article	IF	Citations
181	Hardware and embedded security in the context of internet of things. , 2013, , .		85
182	Is Split Manufacturing Secure?. , 2013, , .		140
183	On design vulnerability analysis and trust benchmarks development. , 2013, , .		183
184	Sneak-Path Testing of Crossbar-Based Nonvolatile Random Access Memories. IEEE Nanotechnology Magazine, 2013, 12, 413-426.	2.0	101
185	Sneak-path Testing of Memristor-based Memories. , 2013, , .		42
186	High-level synthesis for security and trust. , 2013, , .		37
187	VLSI testing based security metric for IC camouflaging. , 2013, , .		33
188	Sneak path testing and fault modeling for multilevel memristor-based memories. , 2013, , .		18
189	New scan-based attack using only the test mode. , 2013, , .		34
190	Security analysis of integrated circuit camouflaging. , 2013, , .		287
191	Shielding heterogeneous MPSoCs from untrustworthy 3PIPs through security-driven task scheduling. , 2013, , .		12
192	Scan attack in presence of mode-reset countermeasure. , 2013, , .		18
193	Recomputing with Permuted Operands: A Concurrent Error Detection Approach. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32, 1595-1608.	2.7	54
194	Security analysis of logic obfuscation. , 2012, , .		366
195	Invariance-based concurrent error detection for advanced encryption standard. , 2012, , .		20
196	Architecture Support for Dynamic Integrity Checking. IEEE Transactions on Information Forensics and Security, 2012, 7, 321-332.	6.9	13
197	Guest Editorial - Integrated Circuit and System Security. IEEE Transactions on Information Forensics and Security, 2012, 7, 1-2.	6.9	3
198	Leveraging Memristive Systems in the Construction of Digital Logic Circuits. Proceedings of the IEEE, 2012, 100, 2033-2049.	21.3	103

#	Article	IF	Citations
199	Balancing performance and fault detection for GPGPU workloads. , 2012, , .		1
200	A Survey of Microarchitecture Support for Embedded Processor Security. , 2012, , .		4
201	Engineering crossbar based emerging memory technologies. , 2012, , .		2
202	A high-performance, low-overhead microarchitecture for secure program execution. , 2012, , .		9
203	Nano-PPUF: A Memristor-Based Security Primitive. , 2012, , .		78
204	An Energy-Efficient Memristive Threshold Logic Circuit. IEEE Transactions on Computers, 2012, 61, 474-487.	3.4	79
205	Trojan Taxonomy. , 2012, , 325-338.		20
206	Security and Testing. , 2012, , 385-409.		3
207	Design and analysis of ring oscillator based Design-for-Trust technique. , 2011, , .		58
208	Security-aware SoC test access mechanisms. , 2011, , .		21
209	Security challenges during VLSI test. , 2011, , .		9
210	Improving GPU Robustness by making use of faulty parts. , 2011, , .		8
211	An Approach to Tolerate Process Related Variations in Memristor-Based Applications. , 2011, , .		31
212	Parallel memristors: Improving variation tolerance in memristive digital circuits. , 2011, , .		4
213	Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges. Computer, 2011, 44, 66-74.	1.1	81
214	Toward Future Systems with Nanoscale Devices: Overcoming the Reliability Challenge. Computer, 2011, 44, 46-53.	1.1	14
215	Scan-based attacks on linear feedback shift register based stream ciphers. ACM Transactions on Design Automation of Electronic Systems, 2011, 16, 1-15.	2.6	35
216	Blue team red team approach to hardware trust assessment. , 2011, , .		26

#	Article	IF	Citations
217	Are hardware performance counters a cost effective way for integrity checking of programs. , 2011, , .		80
218	Trustworthy Hardware: Identifying and Classifying Hardware Trojans. Computer, 2010, 43, 39-46.	1.1	403
219	Compact hardware architectures for BLAKE and LAKE hash functions. , 2010, , .		1
220	SLICED: Slide-based concurrent error detection technique for symmetric block ciphers. , 2010, , .		21
221	Attacks and Defenses for JTAG. IEEE Design and Test of Computers, 2010, 27, 36-47.	1.0	115
222	Memristor based programmable threshold logic array. , 2010, , .		42
223	Sensor physical unclonable functions. , 2010, , .		64
224	Feasibility study of dynamic Trusted Platform Module. , 2010, , .		5
225	Logic Mapping in Crossbar-Based Nanoarchitectures. IEEE Design and Test of Computers, 2009, 26, 68-77.	1.0	30
226	Leveraging CMOS design tools for QCA designs. , 2008, , .		0
227	Efficient construction of minimal Spanning Tree avoiding rectilinear directional obstacles. , 2008, , .		0
228	Fault Tolerant Approaches to Nanoelectronic Programmable Logic Arrays. , 2007, , .		16
229	The Robust QCA Adder Designs Using Composable QCA Building Blocks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2007, 26, 176-183.	2.7	180
230	Power Optimization for Universal Hash Function Data Path Using Divide-and-Concatenate Technique. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2007, 26, 1763-1769.	2.7	0
231	Logic Level Fault Tolerance Approaches Targeting Nanoelectronics PLAs. , 2007, , .		17
232	Design automation for hybrid CMOS-nonoelectronics crossbars. , 2007, , .		3
233	Towards Nanoelectronics Processor Architectures. Journal of Electronic Testing: Theory and Applications (JETTA), 2007, 23, 235-254.	1.2	5
234	Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations. , 2007, , .		0

#	Article	IF	Citations
235	Topology aware mapping of logic functions onto nanowire-based crossbar architectures. , 2006, , .		26
236	Tamper Proofing by Design Using Generalized Involution-Based Concurrent Error Detection for Involutional Substitution Permutation and Feistel Networks. IEEE Transactions on Computers, 2006, 55, 1230-1239.	3.4	4
237	A High-Speed Hardware Architecture for Universal Message Authentication Code. IEEE Journal on Selected Areas in Communications, 2006, 24, 1831-1839.	14.0	9
238	Secure scan. , 2005, , .		29
239	Power optimization for universal hash function data path using divide-and-concatenate technique. , 2005, , .		0
240	Design of a high-performance RSVP-TE hardware signaling accelerator. IEEE Journal on Selected Areas in Communications, 2005, 23, 1588-1595.	14.0	5
241	Divide-and-concatenate: an architecture level optimization technique for universal hash functions. , 2004, , .		6
242	A Heterogeneous Built-In Self-Repair Approach Using System-Level Synthesis Flexibility. IEEE Transactions on Reliability, 2004, 53, 93-101.	4.6	1
243	High speed architectures for Leviathan: a binary tree based stream cipher. Microprocessors and Microsystems, 2004, 28, 573-584.	2.8	1
244	Title is missing!. Mobile Networks and Applications, 2003, 8, 177-185.	3.3	28
245	Selectively breaking data dependences to improve the utilization of idle cycles in algorithm level re-computing data paths. IEEE Transactions on Reliability, 2003, 52, 501-511.	4.6	3
246	Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit RC6 block cipher. Microelectronics Journal, 2003, 34, 31-39.	2.0	3
247	<title>Hardware implementation of a signaling protocol</title>. , 2002, 4874, 174.		9
248	Algorithm level re-computing using implementation diversity: a register transfer level concurrent error detection technique. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2002, 10, 864-875.	3.1	7
249	Introspection. ACM Transactions on Design Automation of Electronic Systems, 2001, 6, 501-515.	2.6	22
250	Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers. , 2001, , .		37
251	Computer aided design of fault-tolerant application specific programmable processors. IEEE Transactions on Computers, 2000, 49, 1272-1284.	3.4	15
252	Power optimization using divide-and-conquer techniques for minimization of the number of operations. ACM Transactions on Design Automation of Electronic Systems, 1999, 4, 405-429.	2.6	1

#	Article	IF	Citations
253	Fault-tolerant vlsi systems. IEEE Transactions on Reliability, 1999, 48, 106-107.	4.6	3
254	Versatile BIST: An Integrated Approach to On-line/Off-line BIST for Data-Dominated Architectures. Journal of Electronic Testing: Theory and Applications (JETTA), 1998, 13, 189-200.	1.2	2
255	Automatic synthesis of self-recovering VLSI systems. IEEE Transactions on Computers, 1996, 45, 131-142.	3.4	55
256	Time-constrained scheduling during high-level synthesis of fault-secure VLSI digital signal processors. IEEE Transactions on Reliability, 1996, 45, 404-412.	4.6	26
257	Optimal algorithms for synthesis of reliable application-specific heterogeneous multiprocessors. IEEE Transactions on Reliability, 1995, 44, 603-613.	4.6	9
258	?â„°â„±ect ?olerant layout synthesis. International Journal of Electronics, 1994, 76, 1121-1133.	1.4	3
259	Synthesis of fault-tolerant and real-time microarchitectures. Journal of Systems and Software, 1994, 25, 73-84.	4.5	4
260	Coactive scheduling and checkpoint determination during high level synthesis of self-recovering microarchitectures. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 1994, 2, 304-311.	3.1	38
261	ALPS. , 1991, , .		2
262	Standard seven segmented display for Burmese numerals. IEEE Transactions on Consumer Electronics, 1990, 36, 959-961.	3.6	3
263	Low cost concurrent error detection for the advanced encryption standard. , 0, , .		84