Yier Jin

List of Publications by Year
in descending order

171	4,473	394421	276875
papers	citations	19 h-index	41 g-index

174	174	174	2425
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems, 2015, 1, 99-109.	2.4	242
2	AppSAT: Approximately deobfuscating integrated circuits. , 2017, , .		215
3	Hardware Trojan detection using path delay fingerprint. , 2008, , .		183
4	Security analysis on consumer and industrial IoT devices. , 2016, , .		168
5	Experiences in Hardware Trojan design and implementation. , 2009, , .		165
6	Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition. IEEE Transactions on Information Forensics and Security, 2012, 7, 25-40.	6.9	143
7	Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. Journal of Hardware and Systems Security, 2018, 2, 97-110.	1.3	128
8	HAFIX. , 2015, , .		119
9	Cyclic Obfuscation for Creating SAT-Unresolvable Circuits. , 2017, , .		116
10	Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 2939-2948.	3.1	116
11	Hardware Trojans in Wireless Cryptographic ICs. IEEE Design and Test of Computers, 2010, 27, 26-35.	1.0	108
12	The Changing Computing Paradigm With Internet of Things: A Tutorial Introduction. IEEE Design and Test, 2016, 33, 76-96.	1.2	83
13	Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 1506-1519.	3.1	81
14	Survey of machine learning methods for detecting false data injection attacks in power systems. IET Smart Grid, 2020, 3, 581-595.	2.2	74
15	Provably secure camouflaging strategy for IC protection. , 2016, , .		73
16	Introduction to Cyber-Physical System Security: A Cross-Layer Perspective. IEEE Transactions on Multi-Scale Computing Systems, 2017, 3, 215-227.	2.4	66
17	Emerging Technology-Based Design of Primitives for Hardware Security. ACM Journal on Emerging Technologies in Computing Systems, 2017, 13, 1-19.	2.3	65
18	IP Protection and Supply Chain Security through Logic Obfuscation. ACM Transactions on Design Automation of Electronic Systems, 2019, 24, 1-36.	2.6	61

#	Article	IF	Citations
19	Revisit sequential logic obfuscation: Attacks and defenses. , 2017, , .		59
20	KC2: Key-Condition Crunching for Fast Sequential Circuit Deobfuscation. , 2019, , .		59
21	Pre-silicon security verification and validation. , 2015, , .		57
22	CloudLeak: Large-Scale Deep Learning Models Stealing Through Adversarial Examples. , 2020, , .		57
23	Robust Adversarial Objects against Deep Learning Models. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34, 954-962.	4.9	55
24	Proof carrying-based information flow tracking for data secrecy protection and hardware trust. , 2012, , .		52
25	ATRIUM: Runtime attestation resilient under memory attacks. , 2017, , .		52
26	Introduction to Hardware Security. Electronics (Switzerland), 2015, 4, 763-784.	3.1	51
27	DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage. , 2020, , .		51
28	Cyber-physical systems: A security perspective. , 2015, , .		50
29	Netlist reverse engineering for high-level functionality reconstruction. , 2016, , .		50
30	Leveraging Emerging Technology for Hardware Security - Case Study on Silicon Nanowire FETs and Graphene SymFETs. , 2014, , .		47
31	On the Approximation Resiliency of Logic Locking and IC Camouflaging Schemes. IEEE Transactions on Information Forensics and Security, 2019, 14, 347-359.	6.9	46
32	Enabling Security-Enhanced Attestation With Intel SGX for Remote Terminal and IoT. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 88-96.	2.7	44
33	Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation. , 2013, , .		43
34	Cross-Lock. , 2018, , .		41
35	Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing. , 2013, , .		40
36	An End-to-End View of IoT Security and Privacy. , 2017, , .		38

#	Article	IF	Citations
37	Development and Evaluation of Hardware Obfuscation Benchmarks. Journal of Hardware and Systems Security, 2018, 2, 142-161.	1.3	38
38	Scalable SoC trust verification using integrated theorem proving and model checking. , 2016, , .		36
39	Beyond the Interconnections: Split Manufacturing in RF Designs. Electronics (Switzerland), 2015, 4, 541-564.	3.1	35
40	Strategy without tactics. , 2016, , .		35
41	Gate-level netlist reverse engineering for hardware security: Control logic register identification. , 2016, , .		34
42	Provably Secure Camouflaging Strategy for IC Protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 1399-1412.	2.7	32
43	Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs. IEEE Transactions on Emerging Topics in Computing, 2017, 5, 340-352.	4.6	31
44	Security analysis and enhancement of model compressed deep learning systems under adversarial attacks. , 2018, , .		29
45	A proof-carrying based framework for trusted microprocessor IP. , 2013, , .		28
46	RTL-PSC: Automated Power Side-Channel Leakage Assessment at Register-Transfer Level. , 2019, , .		28
47	On the Impossibility of Approximation-Resilient Circuit Locking. , 2019, , .		28
48	FIGHT-Metric. , 2014, , .		27
49	Estimation of Safe Sensor Measurements of Autonomous System Under Attack. , 2017, , .		27
50	QIF-Verilog: Quantitative Information-Flow based Hardware Description Languages for Pre-Silicon Security Assessment. , 2019, , .		27
51	Exposing vulnerabilities of untrusted computing platforms. , 2012, , .		26
52	Enhancing security via provably trustworthy hardware intellectual property. , 2011, , .		25
53	Invited - Can IoT be secured. , 2016, , .		24
54	Design-for-Security vs. Design-for-Testability: A Case Study on DFT Chain in Cryptographic Circuits. , 2014, , .		23

#	Article	IF	Citations
55	Security policy enforcement in modern SoC designs. , 2015, , .		21
56	Enhancing Hardware Security with Emerging Transistor Technologies. , 2016, , .		21
57	MT-spike: A multilayer time-based spiking neuromorphic architecture with temporal error backpropagation. , 2017, , .		21
58	Security for safety. , 2018, , .		21
59	R2D2: Runtime reassurance and detection of A2 Trojan. , 2018, , .		19
60	Security of emerging non-volatile memories: Attacks and defenses. , 2016, , .		18
61	Data Secrecy Protection Through Information Flow Tracking in Proof-Carrying Hardware IPâ€"Part I: Framework Fundamentals. IEEE Transactions on Information Forensics and Security, 2017, 12, 2416-2429.	6.9	18
62	Power-based Side-Channel Instruction-level Disassembler. , 2018, , .		18
63	Eliminating the Hardware-Software Boundary: A Proof-Carrying Approach for Trust Evaluation on Computer Systems. IEEE Transactions on Information Forensics and Security, 2017, 12, 405-417.	6.9	15
64	The Old Frontier of Reverse Engineering: Netlist Partitioning. Journal of Hardware and Systems Security, 2018, 2, 201-213.	1.3	15
65	Power-based side-channel instruction-level disassembler. , 2018, , .		15
66	On-Chip Analog Trojan Detection Framework for Microprocessor Trustworthiness. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019, 38, 1820-1830.	2.7	15
67	When Capacitors Attack: Formal Method Driven Design and Detection of Charge-Domain Trojans. , 2019, , .		15
68	SoC interconnection protection through formal verification. The Integration VLSI Journal, 2019, 64, 143-151.	2.1	15
69	ReGDS: A Reverse Engineering Framework from GDSII to Gate-level Netlist. , 2020, , .		15
70	DFTT: Design for Trojan Test. , 2010, , .		14
71	Reliable and high performance STT-MRAM architectures based on controllable-polarity devices. , 2015, , .		14
72	Security Challenges in CPS and IoT: From End-Node to the System. , 2016, , .		14

#	Article	IF	Citations
73	Automatic Code Converter Enhanced PCH Framework for SoC Trust Verification. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3390-3400.	3.1	14
74	SIN2: Stealth infection on neural network â€" A low-cost agile neural Trojan attack methodology. , 2018, , .		14
75	IcySAT: Improved SAT-based Attacks on Cyclic Locked Circuits. , 2019, , .		13
76	TimingSAT: Decamouflaging Timing-based Logic Obfuscation. , 2018, , .		12
77	Design for EM Side-Channel Security through Quantitative Assessment of RTL Implementations. , 2020, , .		12
78	Audio Adversarial Examples Generation with Recurrent Neural Networks. , 2020, , .		12
79	Security validation in IoT space. , 2016, , .		11
80	Data Secrecy Protection Through Information Flow Tracking in Proof-Carrying Hardware IPâ€"Part II: Framework Automation. IEEE Transactions on Information Forensics and Security, 2017, 12, 2430-2443.	6.9	11
81	LAZARUS: Practical Side-Channel Resilient Kernel-Space Randomization. Lecture Notes in Computer Science, 2017, , 238-258.	1.3	11
82	Hardware-Assisted Cybersecurity for IoT Devices. , 2017, , .		11
83	Security and Privacy in IoT Era. , 2017, , 351-378.		11
84	RELIC-FUN: Logic Identification through Functional Signal Comparisons. , 2020, , .		11
85	A Novel TIGFET-based DFF Design for Improved Resilience to Power Side-Channel Attacks. , 2020, , .		11
86	EM Side Channels in Hardware Security: Attacks and Defenses. IEEE Design and Test, 2022, 39, 100-111.	1.2	11
87	Implementation of SMS4 Block Cipher on FPGA. , 2006, , .		10
88	Low complexity bit parallel multiplier for generated by equally-spaced trinomials. Information Processing Letters, 2008, 107, 211-215.	0.6	10
89	NETA. , 2019, , .		10
90	Beyond Digital Domain: Fooling Deep Learning Based Recognition System in Physical World. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34, 1088-1095.	4.9	10

#	Article	IF	Citations
91	On Sensor Security in the Era of IoT and CPS. SN Computer Science, 2021, 2, 1.	3.6	10
92	PowerScout: A Security-Oriented Power Delivery Network Modeling Framework for Cross-Domain Side-Channel Analysis. , 2020, , .		10
93	Impact assessment of net metering on smart home cyberattack detection. , 2015, , .		9
94	Hardware Security Challenges Beyond CMOS: Attacks and Remedies. , 2016, , .		9
95	Circuit Obfuscation and Oracle-guided Attacks. , 2017, , .		9
96	Towards Hardware-Assisted Security for IoT Systems. , 2019, , .		9
97	Resilient Distributed Filter for State Estimation of Cyber-Physical Systems Under Attack. , 2019, , .		9
98	Fast Attack-Resilient Distributed State Estimator for Cyber-Physical Systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 3555-3565.	2.7	9
99	Design and Analysis of Secure Distributed Estimator for Vehicular Platooning in Adversarial Environment. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 3418-3429.	8.0	9
100	Cross-Device Profiled Side-Channel Attacks using Meta-Transfer Learning. , 2021, , .		9
101	Runtime Trust Evaluation and Hardware Trojan Detection Using On-Chip EM Sensors. , 2020, , .		9
102	Quantifying trust in autonomous system under uncertainties. , 2016, , .		8
103	IP protection through gate-level netlist security enhancement. The Integration VLSI Journal, 2017, 58, 563-570.	2.1	8
104	CAD4EM-P: Security-Driven Placement Tools for Electromagnetic Side Channel Protection. , 2019, , .		8
105	Invited - Can IoT be secured. , 2016, , .		7
106	Panel Security and Privacy in the Age of Internet of Things. , 2016, , .		7
107	Device attestation: Past, present, and future. , 2018, , .		7
108	Robust Roadside Physical Adversarial Attack Against Deep Learning in Lidar Perception Modules. , 2021, , .		7

#	Article	IF	Citations
109	A 22-nm 1-Mb 1024-b Read Data-Protected STT-MRAM Macro With Near-Memory Shift-and-Rotate Functionality and 42.6-GB/s Read Bandwidth for Security-Aware Mobile Device. IEEE Journal of Solid-State Circuits, 2022, 57, 1936-1949.	5.4	7
110	Leverage Emerging Technologies For DPA-Resilient Block Cipher Design. , 2016, , .		7
111	A Review and Comparison of AI-enhanced Side Channel Analysis. ACM Journal on Emerging Technologies in Computing Systems, 2022, 18, 1-20.	2.3	7
112	Hardware-software collaboration for secure coexistence with kernel extensions. ACM SIGAPP Applied Computing Review: A Publication of the Special Interest Group on Applied Computing, 2014, 14, 22-35.	0.9	6
113	PT-spike: A precise-time-dependent single spike neuromorphic architecture with efficient supervised learning. , 2018, , .		6
114	Security-Driven Placement and Routing Tools for Electromagnetic Side-Channel Protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1077-1089.	2.7	6
115	How Secure Is Split Manufacturing in Preventing Hardware Trojan?. ACM Transactions on Design Automation of Electronic Systems, 2020, 25, 1-23.	2.6	6
116	Post-deployment trust evaluation in wireless cryptographic ICs. , 2012, , .		5
117	A post-deployment IC trust evaluation architecture. , 2013, , .		5
118	Automatic RTL-to-Formal Code Converter for IP Security Formal Verification. , 2016, , .		5
119	Emerging challenges in cyber-physical systems: A balance of performance, correctness, and security. , 2016, , .		5
120	HA2lloc. , 2017, , .		5
121	Hardware control flow integrity. , 2018, , 181-210.		5
122	Automatic On-Chip Clock Network Optimization for Electromagnetic Side-Channel Protection. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11, 371-382.	3.6	5
123	Towards scalable, secure, and smart mission-critical IoT systems. , 2021, , .		5
124	Hardware Trojan Detection in Analog/RF Integrated Circuits. , 2016, , 241-268.		5
125	A statistical STT-RAM retention model for fast memory subsystem designs. , 2017, , .		4
126	Hardware Trojan Detection and Functionality Determination for Soft IPs. , 2018, , .		4

#	Article	IF	Citations
127	Hardware and Software Co-Verification from Security Perspective. , 2019, , .		4
128	PCBench. , 2021, , .		4
129	Design for Hardware Trust. , 2012, , 365-384.		4
130	EDA tools trust evaluation through security property proofs. , 2014, , .		3
131	EDA tools trust evaluation through security property proofs. , 2014, , .		3
132	Hierarchy-Preserving Formal Verification Methods for Pre-silicon Security Assurance. , 2015, , .		3
133	How secure is split manufacturing in preventing hardware trojan?. , 2016, , .		3
134	Dynamic Information Flow Tracking: Taxonomy, Challenges, and Opportunities. Micromachines, 2021, 12, 898.	2.9	3
135	Real-time trust evaluation in integrated circuits. , 2014, , .		3
136	LAHEL: Lightweight Attestation Hardening Embedded Devices using Macrocells. , 2020, , .		3
137	MITOS: Optimal Decisioning for the Indirect Flow Propagation Dilemma in Dynamic Information Flow Tracking Systems. , 2020, , .		3
138	Real-time trust evaluation in integrated circuits. , 2014, , .		2
139	Hardware Design and Verification Techniques for Supply Chain Risk Mitigation. , 2015, , .		2
140	Guest Editorial: Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 144-145.	2.4	2
141	Exploitations of wireless interfaces via network scanning. , 2017, , .		2
142	Approximate Power Grid Protection Against False Data Injection Attacks. , 2017, , .		2
143	PCH framework for IP runtime security verification. , 2017, , .		2
144	SaeCAS: Secure Authenticated Execution Using CAM-Based Vector Storage. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 4078-4089.	2.7	2

#	Article	IF	Citations
145	Security Oriented Design Framework for EM Side-Channel Protection in RTL Implementations. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 41, 2421-2434.	2.7	2
146	IP Trust: The Problem and Design/Validation-Based Solution. , 2017, , 49-65.		2
147	WaLo: Security Primitive Generator for RT-Level Logic Locking and Watermarking. , 2020, , .		2
148	Building a Low-Cost and State-of-the-Art IoT Security Hands-On Laboratory. IFIP Advances in Information and Communication Technology, 2020, , 289-306.	0.7	2
149	3D-Adv: Black-Box Adversarial Attacks against Deep Learning Models through 3D Sensors. , 2021, , .		2
150	Quantifying Rowhammer Vulnerability for DRAM Security. , 2021, , .		2
151	CHIMERA: A Hybrid Estimation Approach to Limit the Effects of False Data Injection Attacks. , 2021, , .		2
152	FineDIFT: Fine-Grained Dynamic Information Flow Tracking for Data-Flow Integrity Using Coprocessor. IEEE Transactions on Information Forensics and Security, 2022, 17, 559-573.	6.9	2
153	Development and Validation of a Two-Step Predictive Risk Stratification Model for Coronavirus Disease 2019 In-hospital Mortality: A Multicenter Retrospective Cohort Study. Frontiers in Medicine, 2022, 9, 827261.	2.6	2
154	Design of Random Number Generation Algorithm. , 2006, , .		1
155	Unbalanced Exponent Modular Reduction over Binary Field and Its Implementation. , 0, , .		1
156	Is single-scheme Trojan prevention sufficient?. , 2011, , .		1
157	PSCML: Pseudo-Static Current Mode Logic. , 2011, , .		1
158	IP Trust Validation Using Proof-Carrying Hardware. , 2017, , 207-225.		1
159	RERTL: Finite State Transducer Logic Recovery at Register Transfer Level. , 2019, , .		1
160	RADM. , 2021, , .		1
161	Protecting Platoons from Stealthy Jamming Attack. , 2020, , .		1
162	In Praise of Exact-Functional-Secrecy in Circuit Locking. IEEE Transactions on Information Forensics and Security, 2021, 16, 5225-5238.	6.9	1

#	Article	IF	Citations
163	Circuit Deobfuscation from Power Side-Channels using Pseudo-Boolean SAT. , 2021, , .		1
164	IP-Tag: Tag-Based Runtime 3PIP Hardware Trojan Detection in SoC Platforms. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, 42, 68-81.	2.7	1
165	Graph Neural Network based Hardware Trojan Detection at Intermediate Representative for SoC Platforms. , 2022, , .		1
166	Revisiting scalable modular multiplication over GF(2/sup m/) for elliptic curve cryptography. , 2006, , .		0
167	Voting system design pitfalls: Vulnerability analysis and exploitation of a model platform. , 2016, , .		0
168	Guest Editorial: Security Challenges in the IoT Regime. Journal of Hardware and Systems Security, 2017, 1, 297-297.	1.3	0
169	Interconnect Estimation for Mesh-Based Reconfigurable Computing. Lecture Notes in Computer Science, 2006, , 766-775.	1.3	0
170	Fuzzing Hardware: Faith or Reality? : Invited Paper. , 2021, , .		0
171	Inter-IP Malicious Modification Detection through Static Information Flow Tracking. , 2022, , .		0