Jiliang Zhang

List of Publications by Year
in descending order

35 papers	1,083 citations	471477 17 h-index	642715 23 g-index
35 all docs	35 docs citations	35 times ranked	902 citing authors

#	Article	IF	Citations
1	A Practical Logic Obfuscation Technique for Hardware Security. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2016, 24, 1193-1197.	3.1	121
2	A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing. IEEE Transactions on Information Forensics and Security, 2015, 10, 1137-1150.	6.9	107
3	Physical Unclonable Function-Based Key Sharing via Machine Learning for IoT Security. IEEE Transactions on Industrial Electronics, 2020, 67, 7025-7033.	7.9	106
4	Approximation Attacks on Strong PUFs. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39, 2138-2151.	2.7	87
5	Set-Based Obfuscation for Strong PUFs Against Machine Learning Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68, 288-300.	5.4	66
6	Adversarial Examples: Opportunities and Challenges. IEEE Transactions on Neural Networks and Learning Systems, 2019, 31, 1-16.	11.3	65
7	Voltage Over-Scaling-Based Lightweight Authentication for IoT Security. IEEE Transactions on Computers, 2022, 71, 323-336.	3.4	51
8	Recent Attacks and Defenses on FPGA-based Systems. ACM Transactions on Reconfigurable Technology and Systems, 2019, 12, 1-24.	2.5	49
9	A novel method for malware detection on ML-based visualization technique. Computers and Security, 2020, 89, 101682.	6.0	43
10	A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. Tsinghua Science and Technology, 2021, 26, 36-47.	6.1	43
11	HCIC: Hardware-Assisted Control-Flow Integrity Checking. IEEE Internet of Things Journal, 2019, 6, 458-471.	8.7	41
12	T2FA: Transparent Two-Factor Authentication. IEEE Access, 2018, 6, 32677-32686.	4.2	38
13	Frequency Offset-Based Ring Oscillator Physical Unclonable Function. IEEE Transactions on Multi-Scale Computing Systems, 2018, 4, 711-721.	2.4	34
14	Control Flow Integrity Based on Lightweight Encryption Architecture. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 1358-1369.	2.7	29
15	A Double-Node-Upset Self-Recoverable Latch Design for High Performance and Low Power Application. IEEE Transactions on Circuits and Systems II: Express Briefs, 2019, 66, 287-291.	3.0	29
16	Design and Implementation of a Delay-Based PUF for FPGA IP Protection. , 2013, , .		27
17	Reconfigurable Binding against FPGA Replay Attacks. ACM Transactions on Design Automation of Electronic Systems, 2015, 20, 1-20.	2.6	24
18	A survey on security and trust of FPGA-based systems. , 2014, , .		19

#	Article	IF	Citations
19	Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 1520-1527.	3.1	19
20	Application of Linear Predictive Coding for Doppler Through-Wall Radar Target Tracking. IEEE Geoscience and Remote Sensing Letters, 2015, 12, 1317-1321.	3.1	16
21	Efficient verification of IP watermarks in FPGA designs through lookup table content extracting. IEICE Electronics Express, 2012, 9, 1735-1741.	0.8	12
22	Echo Interference Suppression Approach for Doppler Through-Wall Radar. IEEE Sensors Journal, 2015, 15, 3395-3402.	4.7	9
23	Micro-architectural Cache Side-Channel Attacks and Countermeasures. , 2021, , .		8
24	Improving the reliability of RO PUF using frequency offset. , 2014, , .		7
25	Reliable and Anti-cloning PUFs Based on Configurable Ring Oscillators. , 2015, , .		6
26	STT-MRAM-Based Reliable Weak PUF. IEEE Transactions on Computers, 2022, 71, 1564-1574.	3.4	6
27	Machine Learning Attacks on Voltage Over-scaling-based Lightweight Authentication. , 2018, , .		5
28	CT PUF: Configurable Tristate PUF against Machine Learning Attacks. , 2020, , .		4
29	Adversarial Hardware With Functional and Topological Camouflage. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 1685-1689.	3.0	3
30	Lightweight and Secure Branch Predictors against Spectre Attacks. , 2022, , .		3
31	Binding Hardware IPs to Specific FPGA Device via Inter-twining the PUF Response with the FSM of Sequential Circuits. , 2013, , .		2
32	CRAlert: Hardware-Assisted Code Reuse Attack Detection. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69, 1607-1611.	3.0	2
33	HRAE: Hardware-assisted Randomization against Adversarial Example Attacks. , 2020, , .		2
34	TimFastPlace: Critical-path based timing driven FastPlace. IEICE Electronics Express, 2012, 9, 1310-1315.	0.8	0
35	Prediction Stability: A New Metric for Quantitatively Evaluating DNN Outputs. , 2020, , .		0