Farinaz Koushanfar

List of Publications by Year
in descending order

208 papers	9,545 citations	279798 23 h-index	133252 59 g-index
209 all docs	209 docs citations	209 times ranked	4326 citing authors

#	Article	IF	Citations
1	A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design and Test of Computers, 2010, 27, 10-25.	1.0	1,034
2	Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE, 2014, 102, 1126-1141.	21.3	873
3	Exposure in wireless Ad-Hoc sensor networks. , 2001, , .		554
4	A Primer on Hardware Security: Models, Methods, and Metrics. Proceedings of the IEEE, 2014, 102, 1283-1295.	21.3	471
5	EPIC. , 2008, , .		417
6	Ending Piracy of Integrated Circuits. Computer, 2010, 43, 30-38.	1.1	277
7	Lightweight secure PUFs. , 2008, , .		225
8	Chameleon. , 2018, , .		225
9	Techniques for Design and Implementation of Secure Reconfigurable PUFs. ACM Transactions on Reconfigurable Technology and Systems, 2009, 2, 1-33.	2.5	159
10	Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 37-49.	4.6	158
11	Exposure in Wireless Sensor Networks: Theory and Practical Solutions. Wireless Networks, 2002, 8, 443-454.	3.0	156
12	Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching. , 2012, , .		153
13	Deepsecure. , 2018, , .		137
14	DeepInspect: A Black-box Trojan Detection and Mitigation Framework for Deep Neural Networks. , 2019, , .		136
15	Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management. IEEE Transactions on Information Forensics and Security, 2012, 7, 51-63.	6.9	132
16	Heart-to-heart (H2H). , 2013, , .		132
17	Testing Techniques for Hardware Security. , 2008, , .		131
18	FPGA PUF using programmable delay lines. , 2010, , .		118

#	Article	IF	Citations
19	TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits. , 2015, , .		117
20	Behavioral synthesis techniques for intellectual property protection. ACM Transactions on Design Automation of Electronic Systems, 2005, 10, 523-545.	2.6	115
21	EPIC: Ending Piracy of Integrated Circuits. , 2008, , .		107
22	Remote activation of ICs for piracy prevention and digital right management. IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, 2007, , .	0.0	102
23	A Unified Framework for Multimodal Submodular Integrated Circuits Trojan Detection. IEEE Transactions on Information Forensics and Security, 2011, 6, 162-174.	6.9	101
24	Novel Techniques for High-Sensitivity Hardware Trojan Detection Using Thermal and Power Maps. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33, 1792-1805.	2.7	97
25	Security Based on Physical Unclonability and Disorder. , 2012, , 65-102.		90
26	Efficient Power and Timing Side Channels for Physical Unclonable Functions. Lecture Notes in Computer Science, 2014, , 476-492.	1.3	89
27	Hardware metering. , 2001, , .		87
28	DeepSigns. , 2019, , .		86
29	A Taxonomy of Attacks on Federated Learning. IEEE Security and Privacy, 2021, 19, 20-28.	1.2	80
30	Invited - Things, trouble, trust. , 2016, , .		77
31	DeepMarks. , 2019, , .		77
32	FPGA-Based True Random Number Generation Using Circuit Metastability with Adaptive Feedback Control. Lecture Notes in Computer Science, 2011, , 17-32.	1.3	75
33	Consistency-based characterization for IC Trojan detection. , 2009, , .		72
34	ReBNet: Residual Binarized Neural Network. , 2018, , .		71
35	DeepSecure: Scalable Provably-Secure Deep Learning. , 2018, , .		66
36	PUFatt. , 2014, , .		64

#	Article	IF	Citations
37	Trusted Integrated Circuits: A Nondestructive Hidden Characteristics Extraction Approach. Lecture Notes in Computer Science, 2008, , 102-117.	1.3	60
38	Time-Bounded Authentication of FPGAs. IEEE Transactions on Information Forensics and Security, 2011, 6, 1123-1135.	6.9	57
39	Automated Synthesis of Optimized Circuits for Secure Computation. , 2015, , .		56
40	A Framework for Collaborative Learning in Secure High-Dimensional Space. , 2019, , .		56
41	Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples. , 2021, , .		55
42	Idetic: A high-level synthesis approach for enabling long computations on transiently-powered ASICs. , 2013, , .		51
43	Intellectual Property Metering. Lecture Notes in Computer Science, 2001, , 81-95.	1.3	51
44	Can EDA combat the rise of electronic counterfeiting?. , 2012, , .		50
45	Robust stable radiometric fingerprinting for wireless devices. , 2009, , .		49
46	LookNN: Neural network with no multiplication. , 2017, , .		48
47	Universal Adversarial Perturbations for Speech Recognition Systems. , 0, , .		46
48	Balancing security and utility in medical devices?. , 2013, , .		45
49	Fault Tolerance in Wireless Sensor Networks. , 2004, , .		45
50	Hardware Trojan horse benchmark via optimal creation and placement of malicious circuitry. , 2012, , .		42
51	High-Sensitivity Hardware Trojan Detection Using Multimodal Characterization. , 2013, , .		41
52	Hardware Metering: A Survey. , 2012, , 103-122.		40
53	CAD-based security, cryptography, and digital rights management. Proceedings - Design Automation Conference, 2007, , .	0.0	39
54	EDA for secure and dependable cybercars. , 2012, , .		36

#	Article	IF	Citations
55	GTX. , 2000, , .		35
56	SparseHD: Algorithm-Hardware Co-optimization for Efficient High-Dimensional Computing. , 2019, , .		34
57	Safe Machine Learning and Defeating Adversarial Attacks. IEEE Security and Privacy, 2019, 17, 31-38.	1.2	34
58	Protecting bus-based hardware IP by secret sharing. , 2008, , .		33
59	Customizing Neural Networks for Efficient FPGA Implementation. , 2017, , .		33
60	Input vector control for post-silicon leakage current minimization in the presence of manufacturing variability. , 2008, , .		32
61	DeLight. , 2016, , .		32
62	Integrated circuits metering for piracy protection and digital rights management. , 2011, , .		31
63	Active control and digital rights management of integrated circuit IP cores. , 2008, , .		30
64	Hierarchical hybrid power supply networks. , 2010, , .		30
65	HypoEnergy. Hybrid supercapacitor-battery power-supply optimization for Energy efficiency. , 2011, , .		30
66	Shielding and securing integrated circuits with sensors. , 2014, , .		30
67	Extended abstract: Designer’s hardware Trojan horse. , 2008, , .		29
68	Extended abstract: Circuit CAD tools as a security threat. , 2008, , .		29
69	DeepFense. , 2018, , .		29
70	Ultra-low power current-based PUF. , 2011, , .		28
71	A Timing Channel Spyware for the CSMA/CA Protocol. IEEE Transactions on Information Forensics and Security, 2013, 8, 477-487.	6.9	28
72	BioChipWork: Reverse Engineering of Microfluidic Biochips. , 2017, , .		28

#	Article	IF	Citations
73	DeepAttest. , 2019, , .		26
74	Coding-based energy minimization for phase change memory. , 2012, , .		25
75	Processor-Based Strong Physical Unclonable Functions With Aging-Based Response Tuning. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 16-29.	4.6	25
76	Provably complete hardware trojan detection using test point insertion. , 2012, , .		23
77	Compacting privacy-preserving k-nearest neighbor search using logic synthesis. , 2015, , .		23
78	A Built-in-Self-Test Scheme for Online Evaluation of Physical Unclonable Functions and True Random Number Generators. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 2-16.	2.4	23
79	ClockPUF: Physical Unclonable Functions Based on Clock Networks. , 2013, , .		22
80	Provably secure obfuscation of diverse watermarks for sequential circuits. , 2010, , .		21
81	SSketch: An Automated Framework for Streaming Sketch-Based Analysis of Big Data on FPGA. , 2015, , .		21
82	Design and Analysis of Secure and Dependable Automotive CPS: A Steer-by-Wire Case Study. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 813-827.	5.4	21
83	Post-silicon timing characterization by compressed sensing. , 2008, , .		19
84	A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design and Test, 2013, , 1-1.	1.2	19
85	Techniques for Foundry Identification. , 2014, , .		19
86	GarbledCPU. , 2016, , .		19
87	SVD-Based Ghost Circuitry Detection. Lecture Notes in Computer Science, 2009, , 221-234.	1.3	19
88	Deep Learning on Private Data. IEEE Security and Privacy, 2019, 17, 54-63.	1.2	18
89	ProFlip: Targeted Trojan Attack with Progressive Bit Flips. , 2021, , .		18
90	BIST-PUF: Online, hardware-based evaluation of physically unclonable circuit identifiers. , 2014, , .		17

#	Article	IF	Citations
91	LaserSPECks:. , 2007, , .		16
92	Rapid FPGA delay characterization using clock synthesis and sparse sampling. , 2010, , .		16
93	CAMsure. Transactions on Embedded Computing Systems, 2017, 16, 1-20.	2.9	16
94	GenUnlock: An Automated Genetic Algorithm Framework for Unlocking Logic Encryption. , 2019, , .		16
95	Gate Characterization Using Singular Value Decomposition: Foundations and Applications. IEEE Transactions on Information Forensics and Security, 2012, 7, 765-773.	6.9	15
96	Chime: Checkpointing Long Computations on Interm ittently Energized IoT Devices. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 277-290.	2.4	15
97	SemiHD: Semi-Supervised Learning Using Hyperdimensional Computing. , 2019, , .		15
98	Noninvasive leakage power tomography of integrated circuits by compressive sensing. , 2008, , .		14
99	Perform-ML. , 2016, , .		14
100	MPCircuits: Optimized Circuit Generation for Secure Multi-Party Computation. , 2019, , .		14
101	Deep Learning Acceleration with Neuron-to-Memory Transformation. , 2020, , .		14
102	Adversarial Reprogramming of Text Classification Neural Networks. , 2019, , .		14
103	Editorial Low-Power, Intelligent, and Secure Solutions for Realization of Internet of Things. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2013, 3, 1-4.	3.6	13
104	FastWave: Accelerating Autoregressive Convolutional Neural Networks on FPGA. , 2019, , .		13
105	CleaNN. , 2020, , .		13
106	FASE: FPGA Acceleration of Secure Function Evaluation. , 2019, , .		12
107	A Unified Submodular Framework for Multimodal IC Trojan Detection. Lecture Notes in Computer Science, 2010, , 17-32.	1.3	12
108	N-variant IC design. , 2008, , .		11

#	Article	IF	Citations
109	Automated checkpointing for enabling intensive applications on energy harvesting devices. , 2013, , .		11
110	Automated Real-Time Analysis of Streaming Big and Dense Data on Reconfigurable Platforms. ACM Transactions on Reconfigurable Technology and Systems, 2016, 10, 1-22.	2.5	11
111	MAXelerator. , 2018, , .		11
112	Peeking Into the Black Box: A Tutorial on Automated Design Optimization and Parameter Search. IEEE Solid-State Circuits Magazine, 2019, 11, 23-28.	0.4	11
113	Learning to manage combined energy supply systems. , 2011, , .		10
114	I Know Where You are. , 2015, , .		10
115	Privacy preserving localization for smart automotive systems. , 2016, , .		10
116	Active Hardware Metering by Finite State Machine Obfuscation. , 2017, , 161-187.		10
117	Deep3. , 2017, , .		10
118	ARM2GC. , 2019, , .		10
119	Can the SHIELD protect our integrated circuits?. , 2014, , .		9
120	20 Years of research on intellectual property protection. , 2017, , .		9
121	ReDCrypt. ACM Transactions on Reconfigurable Technology and Systems, 2018, 11, 1-21.	2.5	9
122	TinyGarble2. , 2020, , .		9
123	Toward Practical Secure Stable Matching. Proceedings on Privacy Enhancing Technologies, 2017, 2017, 62-78.	2.8	9
124	COINN: Crypto/ML Codesign for Oblivious Inference via Neural Networks. , 2021, , .		9
125	Quo vadis, PUF?: Trends and challenges of emerging physical-disorder based security. , 2014, , .		8
126	An Energy-Efficient Last-Level Cache Architecture for Process Variation-Tolerant 3D Microprocessors. IEEE Transactions on Computers, 2015, 64, 2460-2475.	3.4	8

#	Article	IF	Citations
127	CryptoML: Secure outsourcing of big data machine learning applications. , 2016, , .		8
128	GeneCAI. , 2020, , .		8
129	Anti-Collusion Position Estimation in Wireless Sensor Networks. , 2007, , .		7
130	Integrated circuit digital rights management techniques using physical level characterization. , 2011, , .		7
131	High-performance optimizations on tiled many-core embedded systems: a matrix multiplication case study. Journal of Supercomputing, 2013, 66, 431-487.	3.6	7
132	Design and performance analysis of secure and dependable cybercars: A steer-by-wire case study. , 2016, , .		7
133	Privacy-preserving deep learning and inference. , 2018, , .		7
134	On the Application of Binary Neural Networks in Oblivious Inference. , 2021, , .		7
135	Trojan Signatures in DNN Weights. , 2021, , .		7
136	Cross-modal Adversarial Reprogramming. , 2022, , .		7
137	Hybrid heterogeneous energy supply networks. , 2011, , .		6
138	GenMatch: Secure DNA compatibility testing. , 2016, , .		6
139	RISE. Transactions on Embedded Computing Systems, 2017, 16, 1-18.	2.9	6
140	MAXelerator: FPGA Accelerator for Privacy Preserving Multiply-Accumulate (MAC) on Cloud Servers. , 2018, , .		6
141	EncoDeep. Transactions on Embedded Computing Systems, 2020, 19, 1-29.	2.9	6
142	Multisketches. , 2019, , .		6
143	HASHTAG: Hash Signatures for Online Detection of Fault-Injection Attacks on Deep Neural Networks. , 2021, , .		6
144	Guest Editors' Introduction: Confronting the Hardware Trustworthiness Problem. IEEE Design and Test of Computers, 2010, 27, 8-9.	1.0	5

#	Article	IF	Citations
145	PriSearch. , 2017, , .		5
146	TinyDL: Just-in-time deep learning solution for constrained embedded systems. , 2017, , .		5
147	CausaLearn. , 2018, , .		5
148	CuRTAIL: ChaRacterizing and Thwarting AdversarIal Deep Learning. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 736-752.	5.4	5
149	Security of Microfluidic Biochip. ACM Transactions on Design Automation of Electronic Systems, 2020, 25, 1-29.	2.6	5
150	AdaTest: Reinforcement Learning and Adaptive Sampling for On-chip Hardware Trojan Detection. Transactions on Embedded Computing Systems, 2023, 22, 1-23.	2.9	5
151	Techniques for maintaining connectivity in wireless ad-hoc networks under energy constraints. Transactions on Embedded Computing Systems, 2007, 6, 16.	2.9	4
152	LaserSPECks: Laser SPECtroscopic Trace-Gas Sensor Networks - Sensor Integration and Applications. , 2007, , .		4
153	Quo vadis, PUF?: Trends and challenges of emerging physical-disorder based security. , 2014, , .		4
154	Trustworthy Hardware [Scanning the Issue]. Proceedings of the IEEE, 2014, 102, 1123-1125.	21.3	4
155	Evolving EDA beyond its E-roots: An overview. , 2015, , .		4
156	Phase Change Memory Write Cost Minimization by Data Encoding. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2015, 5, 51-63.	3.6	4
157	SHAIP. ACM Transactions on Design Automation of Electronic Systems, 2018, 23, 1-20.	2.6	4
158	AdaNS: Adaptive Non-Uniform Sampling for Automated Design of Compact DNNs. IEEE Journal on Selected Topics in Signal Processing, 2020, 14, 750-764.	10.8	4
159	Peer-to-Peer Variational Federated Learning Over Arbitrary Graphs. IEEE Journal on Selected Areas in Information Theory, 2022, 3, 172-182.	2.5	4
160	MetaCores. , 2001, , .		3
161	Hardware Security: Preparing Students for the Next Design Frontier. , 2007, , .		3
162	N-version temperature-aware scheduling and binding. , 2009, , .		3

#	Article	IF	Citations
163	A queueing theoretic approach for performance evaluation of low-power multi-core embedded systems. Journal of Parallel and Distributed Computing, 2014, 74, 1872-1890.	4.1	3
164	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
165	Enhancing Model Parallelism in Neural Architecture Search for Multidevice System. IEEE Micro, 2020, 40, 46-55.	1.8	3
166	FlowTrojan: Insertion and Detection of Hardware Trojans on Flow-Based Microfluidic Biochips. , 2020, , .		3
167	Developing Privacy-preserving AI Systems: The Lessons learned. , 2020, , .		3
168	SpecMark: A Spectral Watermarking Framework for IP Protection of Speech Recognition Systems. , 0, , .		3
169	Nonparametric Combinatorial Regression for Shape Constrained Modeling. IEEE Transactions on Signal Processing, 2010, 58, 626-637.	5.3	2
170	Hybrid modeling of non-stationary process variations. , 2011, , .		2
171	Trusted Design in FPGAs. , 2012, , 195-229.		2
172	Fine-Grained Voltage Boosting for Improving Yield in Near-Threshold Many-Core Processors. , 2015, , .		2
173	Flexible Transformations For Learning Big Data. , 2015, , .		2
174	Robust privacy-preserving fingerprint authentication. , 2016, , .		2
175	Going deeper than deep learning for massive data analytics under physical constraints. , 2016, , .		2
176	P3. ACM Transactions on Design Automation of Electronic Systems, 2018, 23, 1-19.	2.6	2
177	SimBNN: A Similarity-Aware Binarized Neural Network Acceleration Framework. , 2019, , .		2
178	AHEC: End-to-end Compiler Framework for Privacy-preserving Machine Learning Acceleration. , 2020, , .		2
179	ILP-based engineering change. Proceedings - Design Automation Conference, 2002, , .	0.0	1
180	Integration of Statistical Techniques in the Design Curriculum. , 2007, , .		1

#	Article	IF	Citations
181	(Bio)-behavioral CAD. , 2008, , .		1
182	Challenging benchmark for location discovery in ad hoc networks. , 2008, , .		1
183	Multiple statistical validations for sensor networks optimization. , 2008, , .		1
184	Trusting the open latent IC backdoors. , 2011, , .		1
185	DA systemization of knowledge: A catalog of prior forward-looking initiatives. , 2015, , .		1
186	RankMap: A Framework for Distributed Learning From Dense Data Sets. IEEE Transactions on Neural Networks and Learning Systems, 2018, 29, 2717-2730.	11.3	1
187	Provably Secure Sequential Obfuscation for IC Metering and Piracy Avoidance. IEEE Design and Test, 2021, 38, 51-57.	1.2	1
188	Sensor Network Architecture. , 2004, , .		1
189	D2Cyber: A design automation tool for dependable cybercars. , 2014, , .		1
190	Principal Component Properties of Adversarial Samples. Communications in Computer and Information Science, 2020, , 58-66.	0.5	1
191	Intellectual Property (IP) Protection for Deep Learning and Federated Learning Models. , 2022, , .		1
192	Global error-tolerant algorithms for location discovery in ad-hoc wireless Netoworks. , 2002, , .		0
193	Hop-by-hop or longer hops: The energy perspective. , 2008, , .		0
194	What is hardware security?. ACM SIGDA Newsletter, 2010, 40, 1-1.	0.0	0
195	Real time emulations. , 2010, , .		0
196	CyCAR'2013. , 2013, , .		0
197	Low-power resource binding by postsilicon customization. ACM Transactions on Design Automation of Electronic Systems, 2013, 18, 1-22.	2.6	0
198	D2Cyber: A design automation tool for dependable cybercars. , 2014, , .		0

#	Article	IF	Citations
199	D2CyberSoft: A design automation tool for soft error analysis of Dependable Cybercars. , 2016, , .		0
200	ExtDict: Extensible Dictionaries for Data- and Platform-Aware Large-Scale Learning. , 2017, , .		0
201	ASHES 2017. , 2017, , .		0
202	Assured deep learning. , 2018, , .		0
203	The Fusion of Secure Function Evaluation and Logic Synthesis. IEEE Security and Privacy, 2021, 19, 48-55.	1.2	0
204	Hardware/Algorithm Codesign for Adversarially Robust Deep Learning. IEEE Design and Test, 2021, 38, 31-38.	1.2	0
205	Localized Algorithms for Sensor Networks. , 2004, , .		0
206	SWANN: Small-World Architecture for Fast Convergence of Neural Networks. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11, 575-585.	3.6	0
207	Unified Architectural Support for Secure and Robust Deep Learning. , 2020, , .		0
208	AutoRank: Automated Rank Selection for Effective Neural Network Customization. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2021, 11, 611-619.	3.6	0