Fan Yao

List of Publications by Year
in descending order

34 papers	403 citations	1307594 7 h-index	1372567 10 g-index
36 all docs	36 docs citations	36 times ranked	188 citing authors

#	Article	IF	Citations
1	T-BFA: <u>T</u>argeted <u>B</u>it-<u>F</u>lip Adversarial Weight <u>A</u>ttack. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 44, 7928-7939.	13.9	15
2	LockedDown: Exploiting Contention on Host-GPU PCIe Bus for Fun and Profit. , 2022, , .		2
3	Red Alert for Power Leakage: Exploiting Intel RAPL-Induced Side Channels. , 2021, , .		8
4	Defeating Cache Timing Channels with Hardware Prefetchers. IEEE Design and Test, 2021, 38, 7-14.	1.2	5
5	LADDER: Architecting Content and Location-aware Writes for Crossbar Resistive Memories. , 2021, , .		5
6	Leaking Secrets through Modern Branch Predictor in the Speculative World. IEEE Transactions on Computers, 2021, , 1-1.	3.4	7
7	Seeds of SEED: NMT-Stroke: Diverting Neural Machine Translation through Hardware-based Faults. , 2021, , .		3
8	Seeds of SEED: R-SAW: New Side Channels Exploiting Read Asymmetry in MLC Phase Change Memories. , 2021, , .		2
9	Cache-Zoomer: On-demand High-resolution Cache Monitoring for Security. Journal of Hardware and Systems Security, 2020, 4, 180-195.	1.3	2
10	Inter-task cache interference aware partitioned real-time scheduling. , 2020, , .		10
11	BranchSpec: Information Leakage Attacks Exploiting Speculative Branch Instruction Executions. , 2020, , .		11
12	Leveraging Cache Management Hardware for Practical Defense Against Cache Timing Channel Attacks. IEEE Micro, 2019, 39, 8-16.	1.8	7
13	COTSknight: Practical Defense against Cache Timing Channel Attacks using Cache Monitoring and Partitioning Technologies. , 2019, , .		13
14	XBFS. , 2019, , .		25
15	Negative Correlation, Non-linear Filtering, and Discovering of Repetitiveness for Cache Timing Channel Detection. , 2019, , .		1
16	PowerStar: Improving Power Efficiency in Heterogenous Processors for Bursty Workloads with Approximate Computing. , 2019, , .		2
17	HolDCSim: A Holistic Simulator for Data Centers*. , 2019, , .		2
18	Are Crossbar Memories Secure? New Security Vulnerabilities in Crossbar Memories. IEEE Computer Architecture Letters, 2019, 18, 174-177.	1.5	7

#	Article	IF	Citations
19	Covert Timing Channels Exploiting Cache Coherence Hardware: Characterization and Defense. International Journal of Parallel Programming, 2019, 47, 595-620.	1.5	10
20	PrODACT: Prefetch-Obfuscator to Defend Against Cache Timing Channels. International Journal of Parallel Programming, 2019, 47, 571-594.	1.5	12
21	TS-BatPro: Improving Energy Efficiency in Data Centers by Leveraging Temporalâ€“Spatial Batching. IEEE Transactions on Green Communications and Networking, 2019, 3, 236-249.	5.5	5
22	Are Coherence Protocol States Vulnerable to Information Leakage?. , 2018, , .		64
23	A Noise-resilient Detection Method against Advanced Cache Timing Channel Attack. , 2018, , .		3
24	PopCorns: Power Optimization Using a Cooperative Network-Server Approach for Data Centers. , 2018, , .		4
25	Prefetch-guard: Leveraging hardware prefetches to defend against cache timing channels. , 2018, , .		23
26	Covert Timing Channels Exploiting Non-Uniform Memory Access based Architectures. , 2017, , .		23
27	StatSym: Vulnerable Path Discovery through Statistics-Guided Symbolic Execution. , 2017, , .		19
28	TS-Bat: Leveraging Temporal-Spatial Batching for Data Center Energy Optimization. , 2017, , .		4
29	WASP: Workload Adaptive Energy-Latency Optimization in Server Farms Using Server Low-Power States. , 2017, , .		13
30	SARRE: Semantics-Aware Rule Recommendation and Enforcement for Event Paths on Android. IEEE Transactions on Information Forensics and Security, 2016, 11, 2748-2762.	6.9	18
31	A Dual Delay Timer Strategy for Optimizing Server Farm Energy. , 2015, , .		6
32	A comparative analysis of data center network architectures. , 2014, , .		37
33	JOP-alarm: Detecting jump-oriented programming-based anomalies in applications. , 2013, , .		14
34	Watts-inside: A hardware-software cooperative approach for Multicore Power Debugging. , 2013, , .		5