Omer Reingold

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10646245/publications.pdf

Version: 2024-02-01

45 papers	2,467 citations	471371 17 h-index	434063 31 g-index
45 all docs	45 docs citations	45 times ranked	944 citing authors

#	Article	IF	Citations
1	Undirected connectivity in log-space. Journal of the ACM, 2008, 55, 1-24.	1.8	311
2	Number-theoretic constructions of efficient pseudo-random functions. Journal of the ACM, 2004, 51, 231-262.	1.8	235
3	On the Construction of Pseudorandom Permutations: Lubyâ€"Rackoff Revisited. Journal of Cryptology, 1999, 12, 29-66.	2.1	226
4	Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders. Annals of Mathematics, 2002, 155, 157.	2.1	202
5	Undirected ST-connectivity in log-space. , 2005, , .		163
6	Preserving Statistical Validity in Adaptive Data Analysis. , 2015, , .		101
7	Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions. Journal of Computer and System Sciences, 1999, 58, 336-375.	0.9	88
8	Assignment Testers: Towards a Combinatorial Proof of the PCP Theorem. SIAM Journal on Computing, 2006, 36, 975-1024.	0.8	86
9	Constant-round interactive proofs for delegating computation. , 2016, , .		85
10	Extracting all the Randomness and Reducing the Error in Trevisan's Extractors. Journal of Computer and System Sciences, 2002, 65, 97-128.	0.9	80
11	Extractors. , 2003, , .		75
12	Extracting all the randomness and reducing the error in Trevisan's extractors. , 1999, , .		66
13	Pseudorandom walks on regular digraphs and the RL vs. L problem. , 2006, , .		63
14	Guilt-free data reuse. Communications of the ACM, 2017, 60, 86-93.	3.3	63
15	Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function. SIAM Journal on Computing, 2009, 39, 1153-1218.	0.8	61
16	On recycling the randomness of states in space bounded computation. , 1999, , .		58
17	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		44
18	Derandomized Constructions of k-Wise (Almost) Independent Permutations. Algorithmica, 2009, 55, 113-133.	1.0	44

#	Article	IF	Citations
19	Breaking generalized Diffieâ€“Hellman modulo a composite is no easier than factoring. Information Processing Letters, 1999, 70, 83-87.	0.4	39
20	Efficiency improvements in constructing pseudorandom generators from one-way functions. , 2010, , .		37
21	Pseudorandom Functions and Factoring. SIAM Journal on Computing, 2002, 31, 1383-1404.	0.8	30
22	Derandomized Constructions of k-Wise (Almost) Independent Permutations. Lecture Notes in Computer Science, 2005, , 354-365.	1.0	28
23	Extracting Randomness via Repeated Condensing. SIAM Journal on Computing, 2006, 35, 1185-1209.	0.8	27
24	Finding Collisions in Interactive Protocols---Tight Lower Bounds on the Round and Communication Complexities of Statistically Hiding Commitments. SIAM Journal on Computing, 2015, 44, 193-242.	0.8	26
25	Inaccessible entropy. , 2009, , .		22
26	Pseudo-random functions and factoring (extended abstract). , 2000, , .		19
27	Universal One-Way Hash Functions via Inaccessible Entropy. Lecture Notes in Computer Science, 2010, , 616-637.	1.0	18
28	Constructing Pseudo-Random Permutations with a Prescribed Structure. Journal of Cryptology, 2002, 15, 97-102.	2.1	17
29	Efficiency Improvements in Constructing Pseudorandom Generators from One-Way Functions. SIAM Journal on Computing, 2013, 42, 1405-1430.	0.8	17
30	Partial exposure in large games. Games and Economic Behavior, 2010, 68, 602-613.	0.4	16
31	Fault tolerance in large games. , 2008, , .		15
32	On the Power of the Randomized Iterate. SIAM Journal on Computing, 2011, 40, 1486-1528.	0.8	14
33	Balls and Bins: Smaller Hash Families and Faster Evaluation. SIAM Journal on Computing, 2013, 42, 1030-1050.	0.8	14
34	Fault tolerance in large games. Games and Economic Behavior, 2014, 86, 438-457.	0.4	14
35	Constant-Round Interactive Proofs for Delegating Computation. SIAM Journal on Computing, 2021, 50, STOC16-255-STOC16-340.	0.8	14
36	Completeness in Two-Party Secure Computation: A Computational View. Journal of Cryptology, 2006, 19, 521-552.	2.1	10

#	Article	IF	Citations
37	S-T connectivity on digraphs with a known stationary distribution. ACM Transactions on Algorithms, 2011, 7, 1-21.	0.9	8
38	Improved pseudorandomness for unordered branching programs through local monotonicity. , 2018, , .		7
39	Tight bounds for shared memory systems accessed by Byzantine processes. Distributed Computing, 2005, 18, 99-109.	0.7	6
40	Fast Pseudorandomness for Independence and Load Balancing. Lecture Notes in Computer Science, 2014, , 859-870.	1.0	6
41	Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes. Lecture Notes in Computer Science, 2002, , 222-236.	1.0	4
42	Pseudorandom Graphs in Data Structures. Lecture Notes in Computer Science, 2014, , 943-954.	1.0	4
43	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		2
44	A New Interactive Hashing Theorem. Journal of Cryptology, 2014, 27, 109-138.	2.1	1
45	Derandomization beyond Connectivity: Undirected Laplacian Systems in Nearly Logarithmic Space. SIAM Journal on Computing, 2021, 50, 1892-1922.	0.8	1