Moni Naor

List of Publications by Year
in descending order

97 papers	9,532 citations	71061 41 h-index	58549 82 g-index
100 all docs	100 docs citations	100 times ranked	2668 citing authors

#	Article	IF	Citations
1	Broadcast Encryption. , 1993, , 480-491.		658
2	Revocation and Tracing Schemes for Stateless Receivers. Lecture Notes in Computer Science, 2001, , 41-62.	1.0	650
3	Nonmalleable Cryptography. SIAM Journal on Computing, 2000, 30, 391-437.	0.8	587
4	Bit commitment using pseudorandomness. Journal of Cryptology, 1991, 4, 151-158.	2.1	513
5	Small-Bias Probability Spaces: Efficient Constructions and Applications. SIAM Journal on Computing, 1993, 22, 838-856.	0.8	437
6	Tracing Traitors. Lecture Notes in Computer Science, 1994, , 257-270.	1.0	327
7	Concurrent zero-knowledge. , 1998, , .		263
8	Number-theoretic constructions of efficient pseudo-random functions. Journal of the ACM, 2004, 51, 231-262.	1.8	235
9	On the Construction of Pseudorandom Permutations: Lubyâ€"Rackoff Revisited. Journal of Cryptology, 1999, 12, 29-66.	2.1	226
10	On Cryptographic Assumptions and Challenges. Lecture Notes in Computer Science, 2003, , 96-109.	1.0	222
11	What Can be Computed Locally?. SIAM Journal on Computing, 1995, 24, 1259-1277.	0.8	215
12	Comparing information without leaking it. Communications of the ACM, 1996, 39, 77-85.	3.3	196
13	Implicat Representation of Graphs. SIAM Journal on Discrete Mathematics, 1992, 5, 596-603.	0.4	156
14	The Load, Capacity, and Availability of Quorum Systems. SIAM Journal on Computing, 1998, 27, 423-447.	0.8	146
15	Computationally Secure Oblivious Transfer. Journal of Cryptology, 2005, 18, 1-35.	2.1	140
16	Efficient Cryptographic Schemes Provably as Secure as Subset Sum. Journal of Cryptology, 1996, 9, 199.	2.1	125
17	Efficient cryptographic schemes provably as secure as subset sum. Journal of Cryptology, 1996, 9, 199-216.	2.1	119
18	On Memory-Bound Functions for Fighting Spam. Lecture Notes in Computer Science, 2003, , 426-444.	1.0	119

#	Article	IF	Citations
19	Oblivious Transfer with Adaptive Queries. Lecture Notes in Computer Science, 1999, , 573-590.	1.0	117
20	Perfect Zero-Knowledge Arguments for NP Using Any One-Way Permutation. Journal of Cryptology, 1998, 11, 87-108.	2.1	113
21	Novel architectures for P2P applications. , 2003, , .		112
22	Distributed Pseudo-random Functions and KDCs. Lecture Notes in Computer Science, 1999, , 327-346.	1.0	111
23	Concurrent zero-knowledge. Journal of the ACM, 2004, 51, 851-898.	1.8	108
24	Deniable Ring Authentication. Lecture Notes in Computer Science, 2002, , 481-498.	1.0	108
25	Oblivious Polynomial Evaluation. SIAM Journal on Computing, 2006, 35, 1254-1281.	0.8	99
26	Amortized Communication Complexity. SIAM Journal on Computing, 1995, 24, 736-750.	0.8	90
27	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
28	A Lower Bound on Probabilistic Algorithms for Distributive Ring Coloring. SIAM Journal on Discrete Mathematics, 1991, 4, 409-412.	0.4	83
29	Magic Functions. Journal of the ACM, 2003, 50, 852-921.	1.8	76
30	On Robust Combiners for Oblivious Transfer and Other Primitives. Lecture Notes in Computer Science, 2005, , 96-113.	1.0	73
31	Public-Key Cryptosystems Resilient to Key Leakage. SIAM Journal on Computing, 2012, 41, 772-814.	0.8	71
32	Threshold traitor tracing. Lecture Notes in Computer Science, 1998, , 502-517.	1.0	68
33	Digital signets. , 1996, , .		66
34	Zaps and Their Applications. SIAM Journal on Computing, 2007, 36, 1513-1543.	0.8	66
35	The probabilistic method yields deterministic parallel algorithms. Journal of Computer and System Sciences, 1994, 49, 478-516.	0.9	63
36	Novel architectures for P2P applications. ACM Transactions on Algorithms, 2007, 3, 34.	0.9	61

#	Article	IF	Citations
37	The complexity of online memory checking. Journal of the ACM, 2009, 56, 1-46.	1.8	56
38	On the Compressibility of $mathcal{NP}$ Instances and Cryptographic Applications. SIAM Journal on Computing, 2010, 39, 1667-1713.	0.8	55
39	Backyard Cuckoo Hashing: Constant Worst-Case Operations with a Succinct Representation. , 2010, , .		52
40	Immunizing Encryption Schemes from Decryption Errors. Lecture Notes in Computer Science, 2004, , 342-360.	1.0	51
41	An Optimally Fair Coin Toss. Lecture Notes in Computer Science, 2009, , 1-18.	1.0	50
42	Nonmalleable Cryptography. SIAM Review, 2003, 45, 727-784.	4.2	48
43	Derandomized Constructions of k-Wise (Almost) Independent Permutations. Algorithmica, 2009, 55, 113-133.	1.0	44
44	Coin-Flipping Games Immune against Linear-Sized Coalitions. SIAM Journal on Computing, 1993, 22, 403-417.	0.8	43
45	An Efficient Existentially Unforgeable Signature Scheme and Its Applications. Journal of Cryptology, 1998, 11, 187-208.	2.1	43
46	Is There an Oblivious RAM Lower Bound?. , 2016, , .		43
47	Succinct representation of general unlabeled graphs. Discrete Applied Mathematics, 1990, 28, 303-307.	0.5	41
48	Search Problems in the Decision Tree Model. SIAM Journal on Discrete Mathematics, 1995, 8, 119-132.	0.4	36
49	On the Compressibility of NP Instances and Cryptographic Applications. , 2006, , .		36
50	On fairness in the carpool problem. Journal of Algorithms, 2005, 55, 93-98.	0.9	35
51	Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles. Theory of Computing Systems, 2009, 44, 245-268.	0.7	35
52	Optimal File Sharing in Distributed Networks. SIAM Journal on Computing, 1995, 24, 158-183.	0.8	34
53	Scalable and dynamic quorum systems. , 2003, , .		34
54	Pseudorandom Functions and Factoring. SIAM Journal on Computing, 2002, 31, 1383-1404.	0.8	30

#	Article	IF	Citations
55	Fast Interactive Coding against Adversarial Noise. Journal of the ACM, 2014, 61, 1-30.	1.8	28
56	Derandomized Constructions of k-Wise (Almost) Independent Permutations. Lecture Notes in Computer Science, 2005, , 354-365.	1.0	28
57	How Efficient Can Memory Checking Be?. Lecture Notes in Computer Science, 2009, , 503-520.	1.0	28
58	Basing cryptographic protocols on tamper-evident seals. Theoretical Computer Science, 2010, 411, 1283-1310.	0.5	27
59	Fairness in Scheduling. Journal of Algorithms, 1998, 29, 306-357.	0.9	26
60	Secret-Sharing for NP. Journal of Cryptology, 2017, 30, 444-469.	2.1	25
61	Collision Resistant Hashing for Paranoids: Dealing with Multiple Collisions. Lecture Notes in Computer Science, 2018, , 162-194.	1.0	25
62	An Optimally Fair Coin Toss. Journal of Cryptology, 2016, 29, 491-513.	2.1	23
63	Efficient trace and revoke schemes. International Journal of Information Security, 2010, 9, 411-424.	2.3	22
64	Basing Cryptographic Protocols on Tamper-Evident Seals. Lecture Notes in Computer Science, 2005, , 285-297.	1.0	22
65	Bloom Filters in Adversarial Environments. Lecture Notes in Computer Science, 2015, , 565-584.	1.0	22
66	How to Share a Secret, Infinitely. Lecture Notes in Computer Science, 2016, , 485-514.	1.0	21
67	Sketching in Adversarial Environments. SIAM Journal on Computing, 2011, 40, 1845-1870.	0.8	18
68	Bloom Filters in Adversarial Environments. ACM Transactions on Algorithms, 2019, 15, 1-30.	0.9	18
69	Constructing Pseudo-Random Permutations with a Prescribed Structure. Journal of Cryptology, 2002, 15, 97-102.	2.1	17
70	Physical Zero-Knowledge Proofs of Physical Properties. Lecture Notes in Computer Science, 2014, , 313-336.	1.0	17
71	White-Box vs. Black-Box Complexity of Search Problems: Ramsey and Graph Property Testing. , 2017, , .		17
72	Secret-Sharing for NP. Lecture Notes in Computer Science, 2014, , 254-273.	1.0	15

#	Article	IF	Citations
73	Tight Bounds for Sliding Bloom Filters. Algorithmica, 2015, 73, 652-672.	1.0	13
74	One-bit algorithms. Distributed Computing, 1990, 4, 3-8.	0.7	12
75	Scalable and dynamic quorum systems. Distributed Computing, 2005, 17, 311-322.	0.7	12
76	Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles. Lecture Notes in Computer Science, 2007, , 166-182.	1.0	11
77	White-Box vs. Black-Box Complexity of Search Problems. Journal of the ACM, 2019, 66, 1-28.	1.8	11
78	Non-oblivious hashing. , 1988, , .		10
79	Completeness in Two-Party Secure Computation: A Computational View. Journal of Cryptology, 2006, 19, 521-552.	2.1	10
80	Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. IEEE Transactions on Information Theory, 2008, 54, 2408-2425.	1.5	10
81	Hardness Preserving Reductions via Cuckoo Hashing. Lecture Notes in Computer Science, 2013, , 40-59.	1.0	10
82	How to Share a Secret, Infinitely. IEEE Transactions on Information Theory, 2018, 64, 4179-4190.	1.5	9
83	Adversarial laws of large numbers and optimal regret in online classification. , 2021, , .		9
84	Learning to impersonate. , 2006, , .		7
85	Sketching in adversarial environments. , 2008, , .		7
86	Storing and searching a multikey table. , 1988, , .		6
87	Fault-Tolerant Storage in a Dynamic Environment. Lecture Notes in Computer Science, 2004, , 390-404.	1.0	5
88	The Security of Lazy Users in Out-of-Band Authentication. Lecture Notes in Computer Science, 2018, , 575-599.	1.0	4
89	Games for extracting randomness. Xrds, 2010, 17, 44-48.	0.2	3
90	Hardness-Preserving Reductions via Cuckoo Hashing. Journal of Cryptology, 2019, 32, 361-392.	2.1	3

#	Article	IF	Citations
91	The Dynamic And-Or Quorum System. Lecture Notes in Computer Science, 2005, , 472-486.	1.0	3
92	When Can Limited Randomness Be Used in Repeated Games?. Theory of Computing Systems, 2016, 59, 722-746.	0.7	2
93	Title is missing!. Theory of Computing, 2009, 5, 43-67.	0.3	2
94	On the Decisional Complexity of Problems Over the Reals. Information and Computation, 2001, 167, 27-45.	0.5	0
95	The Family Holiday Gathering Problem or Fair and Periodic Scheduling of Independent Sets. , 2016, , .		0
96	Implementing Huge Sparse Random Graphs. Lecture Notes in Computer Science, 2007, , 596-608.	1.0	0
97	The Security of Lazy Users in Out-of-Band Authentication. ACM Transactions on Privacy and Security, 2020, 23, 1-32.	2.2	0