Oded Goldreich

List of Publications by Year
in descending order

244 papers	21,161 citations	44069 48 h-index	17592 121 g-index
271 all docs	271 docs citations	271 times ranked	4690 citing authors

#	Article	IF	Citations
1	How to construct random functions. Journal of the ACM, 1986, 33, 792-807.	2.2	1,417
2	Software protection and simulation on oblivious RAMs. Journal of the ACM, 1996, 43, 431-473.	2.2	1,109
3	Private information retrieval. Journal of the ACM, 1998, 45, 965-981.	2.2	1,059
4	A randomized protocol for signing contracts. Communications of the ACM, 1985, 28, 637-647.	4.5	948
5	Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. Journal of the ACM, 1991, 38, 690-728.	2.2	802
6	On the (Im)possibility of Obfuscating Programs. Lecture Notes in Computer Science, 2001, , 1-18.	1.3	703
7	Property testing and its connection to learning and approximation. Journal of the ACM, 1998, 45, 653-750.	2.2	702
8	The random oracle methodology, revisited. Journal of the ACM, 2004, 51, 557-594.	2.2	614
9	Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. SIAM Journal on Computing, 1988, 17, 230-261.	1.0	418
10	Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 1994, 7, 1-32.	2.8	414
11	The random oracle methodology, revisited (preliminary version). , 1998, , .		393
12	Simple Constructions of Almost k-wise Independent Random Variables. Random Structures and Algorithms, 1992, 3, 289-304.	1.1	382
13	Free Bits, PCPs, and Nonapproximability---Towards Tight Results. SIAM Journal on Computing, 1998, 27, 804-915.	1.0	354
14	On the time-complexity of broadcast in multi-hop radio networks: An exponential gap between determinism and randomization. Journal of Computer and System Sciences, 1992, 45, 104-126.	1.2	353
15	Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. , 1986, , .		342
16	Adaptively secure multi-party computation. , 1996, , .		334
17	On the (im)possibility of obfuscating programs. Journal of the ACM, 2012, 59, 1-48.	2.2	334
18	On Defining Proofs of Knowledge. , 1992, , 390-420.		285

#	Article	IF	Citations
19	On the Composition of Zero-Knowledge Proof Systems. SIAM Journal on Computing, 1996, 25, 169-192.	1.0	280
20	RSA and Rabin Functions: Certain Parts are as Hard as the Whole. SIAM Journal on Computing, 1988, 17, 194-209.	1.0	275
21	Public-key cryptosystems from lattice reduction problems. Lecture Notes in Computer Science, 1997, , 112-131.	1.3	251
22	On-line/off-line digital signatures. Journal of Cryptology, 1996, 9, 35-67.	2.8	245
23	The bit extraction problem or t-resilient functions. , 1985, , .		241
24	A fair protocol for signing contracts. IEEE Transactions on Information Theory, 1990, 36, 40-46.	2.4	235
25	How To Construct Constant-Round Zero-Knowledge Proof Systems for NP. Journal of Cryptology, 1996, 9, 167.	2.8	187
26	Testing Monotonicity. Combinatorica, 2000, 20, 301-337.	1.2	148
27	On the power of two-point based sampling. Journal of Complexity, 1989, 5, 96-106.	1.3	146
28	On-Line/Off-Line Digital Signatures. , 1989, , 263-275.		144
29	Robust PCPs of Proximity, Shorter PCPs, and Applications to Coding. SIAM Journal on Computing, 2006, 36, 889-974.	1.0	144
30	Session-Key Generation Using Human Passwords Only. Lecture Notes in Computer Science, 2001, , 408-432.	1.3	136
31	How to construct constant-round zero-knowledge proof systems for NP. Journal of Cryptology, 1996, 9, 167-189.	2.8	135
32	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, 1999, , .	0.6	130
33	Asynchronous secure computation. , 1993, , .		121
34	On the theory of average case complexity. Journal of Computer and System Sciences, 1992, 44, 193-219.	1.2	117
35	Three theorems regarding testing graph properties. Random Structures and Algorithms, 2003, 23, 23-57.	1.1	114
36	On the Limits of Nonapproximability of Lattice Problems. Journal of Computer and System Sciences, 2000, 60, 540-563.	1.2	112

#	Article	IF	Citations
37	Resettable zero-knowledge (extended abstract). , 2000, , .		109
38	A Sublinear Bipartiteness Tester for Bounded Degree Graphs. Combinatorica, 1999, 19, 335-373.	1.2	106
39	Everything Provable is Provable in Zero-Knowledge. Lecture Notes in Computer Science, 1990, , 37-56.	1.3	103
40	Locally testable codes and PCPs of almost-linear length. Journal of the ACM, 2006, 53, 558-655.	2.2	96
41	Incremental cryptography and application to virus protection. , 1995, , .		92
42	On the Existence of Pseudorandom Generators. SIAM Journal on Computing, 1993, 22, 1163-1175.	1.0	88
43	On the np-completeness of certain network testing problems. Networks, 1984, 14, 1-24.	2.7	87
44	A trade-off between information and communication in broadcast protocols. Journal of the ACM, 1990, 37, 238-256.	2.2	86
45	A uniform-complexity treatment of encryption and zero-knowledge. Journal of Cryptology, 1993, 6, 21-53.	2.8	84
46	Learning Polynomials with Queries: The Highly Noisy Case. SIAM Journal on Discrete Mathematics, 2000, 13, 535-570.	0.8	82
47	Efficient emulation of single-hop radio network with collision detection on multi-hop radio network with no collision detection. Distributed Computing, 1991, 5, 67-71.	0.8	81
48	Property testing in bounded degree graphs. , 1997, , .		76
49	More Constructions of Lossy and Correlation-Secure Trapdoor Functions. Lecture Notes in Computer Science, 2010, , 279-295.	1.3	74
50	On the time-complexity of broadcast in radio networks: an exponential gap between determinism randomization. , 1987, , .		69
51	Improved Testing Algorithms for Monotonicity. Lecture Notes in Computer Science, 1999, , 97-108.	1.3	68
52	The minimum-length generator sequence problem is NP-hard. Journal of Algorithms, 1981, 2, 311-313.	0.9	67
53	Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. , 1998, , .		64
54	Universal Arguments and their Applications. SIAM Journal on Computing, 2009, 38, 1661-1694.	1.0	64

#	Article	IF	Citations
55	On interactive proofs with a laconic prover. Computational Complexity, 2002, 11, 1-53.	0.3	63
56	Lower bounds for sampling algorithms for estimating the average. Information Processing Letters, 1995, 53, 17-25.	0.6	60
57	On the Cryptographic Applications of Random Functions (Extended Abstract). , 1984, , 276-288.		57
58	On the complexity of interactive proofs with bounded communication. Information Processing Letters, 1998, 67, 205-214.	0.6	57
59	Uniform Generation of NP-Witnesses Using an NP-Oracle. Information and Computation, 2000, 163, 510-526.	0.7	57
60	How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design (Extended Abstract). , 1986, , 171-185.		56
61	The random oracle hypothesis is false. Journal of Computer and System Sciences, 1994, 49, 24-39.	1.2	55
62	On the composition of zero-knowledge proof systems. , 1990, , 268-282.		54
63	Tiny families of functions with random properties: A quality-size trade-off for hashing. Random Structures and Algorithms, 1997, 11, 315-343.	1.1	54
64	Theory of computing. ACM Computing Surveys, 1996, 28, 218.	23.0	54
65	Chinese remaindering with errors. , 1999, , .		53
66	Unbiased bits from sources of weak randomness and probabilistic communication complexity. , 1985, , .		52
67	Robust pcps of proximity, shorter pcps and applications to coding. , 2004, , .		52
68	Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme. , 1986, , 104-110.		52
69	A note on computational indistinguishability. Information Processing Letters, 1990, 34, 277-281.	0.6	46
70	Approximating average parameters of graphs. Random Structures and Algorithms, 2008, 32, 473-493.	1.1	45
71	Cryptography and cryptographic protocols. Distributed Computing, 2003, 16, 177-199.	0.8	42
72	On basing one-way functions on NP-hardness. , 2006, , .		42

#	Article	IF	Citations
73	On Promise Problems: A Survey. Lecture Notes in Computer Science, 2006, , 254-290.	1.3	42
74	Session-Key Generation Using Human Passwords Only. Journal of Cryptology, 2006, 19, 241-340.	2.8	40
75	More Constructions of Lossy and Correlation-Secure Trapdoor Functions. Journal of Cryptology, 2013, 26, 39-74.	2.8	40
76	A Simple Protocol for Signing Contracts. , 1984, , 133-136.		40
77	On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes. Lecture Notes in Computer Science, 2004, , 40-57.	1.3	40
78	Foundations of Cryptography â€“ A Primer. Foundations and Trends in Theoretical Computer Science, 2005, 1, 1-116.	0.3	39
79	Randomness in interactive proofs. Computational Complexity, 1993, 3, 319-354.	0.3	38
80	Efficient approximation of product distributions. Random Structures and Algorithms, 1998, 13, 1-16.	1.1	37
81	Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK and NISZK. Lecture Notes in Computer Science, 1999, , 467-484.	1.3	36
82	On Proximity-Oblivious Testing. SIAM Journal on Computing, 2011, 40, 534-566.	1.0	33
83	On Testing Expansion in Bounded-Degree Graphs. Lecture Notes in Computer Science, 2011, , 68-75.	1.3	33
84	Fault-tolerant Computation in the Full Information Model. SIAM Journal on Computing, 1998, 27, 506-544.	1.0	32
85	Lower bounds for linear locally decodable codes and private information retrieval. Computational Complexity, 2006, 15, 263-296.	0.3	32
86	An improved parallel algorithm for integer GCD. Algorithmica, 1990, 5, 1-10.	1.3	31
87	Almost k-wise independence versus k-wise independence. Information Processing Letters, 2003, 88, 107-110.	0.6	31
88	Interactive proof systems: Provers that never fail and random selection. , 1987, , .		30
89	A theory of goal-oriented communication. Journal of the ACM, 2012, 59, 1-65.	2.2	30
90	DES-like functions can generate the alternating group. IEEE Transactions on Information Theory, 1983, 29, 863-865.	2.4	29

#	Article	IF	Citations
91	On the foundations of modern cryptography. Lecture Notes in Computer Science, 1997, , 46-74.	1.3	28
92	Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier. Lecture Notes in Computer Science, 1999, , 270-287.	1.3	28
93	Enhancements of Trapdoor Permutations. Journal of Cryptology, 2013, 26, 484-512.	2.8	27
94	On Yaoâ€™s XOR-Lemma. Lecture Notes in Computer Science, 2011, , 273-301.	1.3	27
95	The best of both worlds: guaranteeing termination in fast randomized byzantine agreement protocols. Information Processing Letters, 1990, 36, 45-49.	0.6	26
96	A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm. Journal of Cryptology, 1993, 6, 97-116.	2.8	26
97	Electronic Wallet. , 1984, , 383-386.		25
98	Candidate One-Way Functions Based on Expander Graphs. Lecture Notes in Computer Science, 2011, , 76-87.	1.3	25
99	A Combinatorial Consistency Lemma with Application to Proving the PCP Theorem. SIAM Journal on Computing, 2000, 29, 1132-1154.	1.0	24
100	Finding cycles and trees in sublinear time. Random Structures and Algorithms, 2014, 45, 139-184.	1.1	23
101	Self-delegation with controlled propagation â€” or â€” What if you lose your laptop. Lecture Notes in Computer Science, 1998, , 153-168.	1.3	22
102	Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs. Lecture Notes in Computer Science, 1995, , 325-338.	1.3	22
103	Derandomization That Is Rarely Wrong from Short Advice That Is Typically Good. Lecture Notes in Computer Science, 2002, , 209-223.	1.3	22
104	A Sample of Samplers: A Computational Perspective on Sampling. Lecture Notes in Computer Science, 2011, , 302-332.	1.3	21
105	On the Implementation of Huge Random Objects. SIAM Journal on Computing, 2010, 39, 2761-2822.	1.0	20
106	Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art. Lecture Notes in Computer Science, 2011, , 406-421.	1.3	20
107	Electing a leader in a ring with link failures. Acta Informatica, 1987, 24, 79-91.	0.5	18
108	Bounds on tradeoffs between randomness and communication complexity. Computational Complexity, 1993, 3, 141-167.	0.3	18

#	Article	IF	Citations
109	Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle Is NP-Hard. Lecture Notes in Computer Science, 2011, , 1-5.	1.3	18
110	A fair protocol for signing contracts. Lecture Notes in Computer Science, 1985, , 43-52.	1.3	17
111	On proximity oblivious testing. , 2009, , .		17
112	On Testing Computability by Small Width OBDDs. Lecture Notes in Computer Science, 2010, , 574-587.	1.3	17
113	Introduction to Testing Graph Properties. Lecture Notes in Computer Science, 2010, , 105-141.	1.3	16
114	Collision-Free Hashing from Lattice Problems. Lecture Notes in Computer Science, 2011, , 30-39.	1.3	16
115	Computational Sample Complexity. SIAM Journal on Computing, 2000, 29, 854-879.	1.0	15
116	Bounds on 2-Query Codeword Testing. Lecture Notes in Computer Science, 2003, , 216-227.	1.3	15
117	Three XOR-Lemmas â€" An Exposition. Lecture Notes in Computer Science, 2011, , 248-272.	1.3	15
118	On the complexity of computation in the presence of link failures: the case of a ring. Distributed Computing, 1991, 5, 121-131.	0.8	14
119	On Learning and Testing Dynamic Environments. Journal of the ACM, 2017, 64, 1-90.	2.2	14
120	Sparse pseudorandom distributions. Random Structures and Algorithms, 1992, 3, 163-174.	1.1	13
121	Addendum to â€œsimple constructions of almost k-wise independent random variablesâ€• Random Structures and Algorithms, 1993, 4, 119-120.	1.1	13
122	A sublinear bipartiteness tester for bounded degree graphs. , 1998, , .		13
123	Algorithmic Aspects of Property Testing in the Dense Graphs Model. SIAM Journal on Computing, 2011, 40, 376-445.	1.0	13
124	On derandomizing algorithms that err extremely rarely. , 2014, , .		13
125	Counting t-Cliques: Worst-Case to Average-Case Reductions and Direct Interactive Proof Systems. , 2018, , .		13
126	Short Locally Testable Codes and Proofs: A Survey in Two Parts. Lecture Notes in Computer Science, 2010, , 65-104.	1.3	13

#	Article	IF	Citations
127	Hashing Functions can Simplify Zero-Knowledge Protocol Design (too). BRICS Report Series, 1994, 1, .	0.2	13
128	On The Randomness Complexity of Property Testing. Computational Complexity, 2010, 19, 99-133.	0.3	12
129	Tiny families of functions with random properties: A quality-size trade-off for hashing. , 1997, 11, 315.		12
130	In a World of P=BPP. Lecture Notes in Computer Science, 2011, , 191-232.	1.3	12
131	Computational Complexity and Knowledge Complexity. SIAM Journal on Computing, 1998, 27, 1116-1141.	1.0	11
132	The tensor product of two good codes is not necessarily robustly testable. Information Processing Letters, 2012, 112, 351-355.	0.6	11
133	On-Line/Off-Line Digital Signatures. Journal of Cryptology, 1996, 9, 35.	2.8	11
134	Improved Derandomization of BPP Using a Hitting Set Generator. Lecture Notes in Computer Science, 1999, , 131-137.	1.3	10
135	Randomness and Computation. Lecture Notes in Computer Science, 2011, , 507-539.	1.3	10
136	On Constructing 1-1 One-Way Functions. Lecture Notes in Computer Science, 2011, , 13-25.	1.3	9
137	Hierarchy Theorems for Property Testing. Computational Complexity, 2012, 21, 129-192.	0.3	9
138	On the Security of Ping-Pong Protocols when Implemented using the RSA (Extended Abstract). , 1985, , 58-72.		8
139	Tiny families of functions with random properties (preliminary version). , 1994, , .		8
140	On Sample-Based Testers. , 2015, , .		8
141	On Sample-Based Testers. ACM Transactions on Computation Theory, 2016, 8, 1-54.	0.7	8
142	Property Testing in Massive Graphs. Massive Computing, 2002, , 123-147.	0.4	8
143	On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions and Their Benefits. , 2007, , 174-193.		8
144	On Probabilistic versus Deterministic Provers in the Definition of Proofs of Knowledge. Lecture Notes in Computer Science, 2011, , 114-123.	1.3	8

#	Article	IF	Citations
145	A tradeoff between information and communication in broadcast protocols. , 1988, , 369-379.		7
146	The graph clustering problem has a perfect zero-knowledge interactive proof. Information Processing Letters, 1999, 69, 201-206.	0.6	7
147	On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions andÂTheirÂBenefits. Journal of Cryptology, 2010, 23, 1-36.	2.8	7
148	On the possibilities and limitations of pseudodeterministic algorithms. , 2013, , .		7
149	The Bit Security of Modular Squaring given Partial Factorization of the Modulos. , 1985, , 448-457.		7
150	On Interactive Proofs with a Laconic Prover. Lecture Notes in Computer Science, 2001, , 334-345.	1.3	7
151	Simplified Derandomization of BPP Using a Hitting Set Generator. Lecture Notes in Computer Science, 2011, , 59-67.	1.3	7
152	Computational complexity and knowledge complexity (extended abstract). , 1994, , .		6
153	Computational indistinguishability: Algorithms vs. circuits. Theoretical Computer Science, 1998, 191, 215-218.	0.9	6
154	Matrix rigidity of random toeplitz matrices. , 2016, , .		6
155	Matrix rigidity of random Toeplitz matrices. Computational Complexity, 2018, 27, 305-350.	0.3	6
156	Sparse Pseudorandom Distributions. , 1989, , 113-127.		6
157	RSA/Rabin least significant bits are $$ frac{1} {2} + frac{1} {{poly left({log N} ight)}} $$ secure (Extended Abstract). , 1984, , 303-313.		6
158	A Taxonomy of Proof Systems. , 1997, , 109-134.		6
159	The Foundations of Modern Cryptography. Algorithms and Combinatorics, 1999, , 1-37.	0.6	6
160	Notes on Levinâ€™s Theory of Average-Case Complexity. Lecture Notes in Computer Science, 2011, , 233-247.	1.3	6
161	Towards a Theory of Software Protection (Extended Abstract). , 1986, , 426-439.		5
162	On the foundations of cryptography. , 2019, , .		5

#	Article	IF	Citations
163	Efficient approximation of product distributions. , 1998, 13, 1.		5
164	Probabilistic Proof Systems. , 1995, , 1395-1406.		5
165	Proximity Oblivious Testing and the Role of Invariances. Lecture Notes in Computer Science, 2011, , 579-592.	1.3	5
166	Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs. Lecture Notes in Computer Science, 2015, , 666-677.	1.3	5
167	Title is missing!. Theory of Computing, 2012, 8, 231-238.	0.5	5
168	Another Proof That $mathcal{BPP}subseteq mathcal{PH}$ (and More). Lecture Notes in Computer Science, 2011, , 40-53.	1.3	5
169	A combinatorial consistency lemma with application to proving the PCP theorem. Lecture Notes in Computer Science, 1997, , 67-84.	1.3	5
170	Erratum for. , 2010, , .		4
171	On Doubly-Efficient Interactive Proof Systems. Foundations and Trends in Theoretical Computer Science, 2018, 13, 157-246.	0.3	4
172	On the Randomness Complexity of Property Testing. Lecture Notes in Computer Science, 2007, , 509-524.	1.3	4
173	Algorithmic Aspects of Property Testing in the Dense Graphs Model. Lecture Notes in Computer Science, 2010, , 295-305.	1.3	4
174	Basic Facts about Expander Graphs. Lecture Notes in Computer Science, 2011, , 451-464.	1.3	4
175	Hierarchy Theorems for Property Testing. Lecture Notes in Computer Science, 2009, , 504-519.	1.3	4
176	A Brief Introduction to Property Testing. Lecture Notes in Computer Science, 2010, , 1-5.	1.3	4
177	Short Locally Testable Codes and Proofs. Lecture Notes in Computer Science, 2011, , 333-372.	1.3	4
178	Worst-Case to Average-Case Reductions for Subclasses of P. Lecture Notes in Computer Science, 2020, , 249-295.	1.3	4
179	On universal learning algorithms. Information Processing Letters, 1997, 63, 131-136.	0.6	3
180	Special Issue On Worst-case Versus Average-case Complexity Editorsâ€™ Foreword. Computational Complexity, 2007, 16, 325-330.	0.3	3

#	Article	IF	Citations
181	Two-sided error proximity oblivious testing. Random Structures and Algorithms, 2016, 48, 341-383.	1.1	3
182	Strong Locally Testable Codes with Relaxed Local Decoders. ACM Transactions on Computation Theory, 2019, 11, 1-38.	0.7	3
183	Using the FGLSS-Reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs. Lecture Notes in Computer Science, 2011, , 88-97.	1.3	3
184	Bravely, Moderately: A Common Theme in Four Recent Works. Lecture Notes in Computer Science, 2011, , 373-389.	1.3	3
185	Two-Sided Error Proximity Oblivious Testing. Lecture Notes in Computer Science, 2012, , 565-578.	1.3	3
186	Efficient emulation of single-hop radio network with collision detection on multi-hop radio network with no collision detection. Lecture Notes in Computer Science, 1989, , 24-32.	1.3	3
187	On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing. Lecture Notes in Computer Science, 2020, , 87-118.	1.3	3
188	Probabilistic proof systems â€" A survey. Lecture Notes in Computer Science, 1997, , 595-611.	1.3	2
189	Computational Indistinguishability: A Sample Hierarchy. Journal of Computer and System Sciences, 1999, 59, 253-269.	1.2	2
190	Proving Computational Ability. Lecture Notes in Computer Science, 2011, , 6-12.	1.3	2
191	On Learning and Testing Dynamic Environments. , 2014, , .		2
192	Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly. ACM Transactions on Computation Theory, 2015, 7, 1-13.	0.7	2
193	Hierarchy Theorems for Testing Properties in Size-Oblivious Query Complexity. Computational Complexity, 2019, 28, 709-747.	0.3	2
194	Testing graphs in vertex-distribution-free models. , 2019, , .		2
195	Universal locally verifiable codes and 3-round interactive proofs of proximity for CSP. Theoretical Computer Science, 2021, 878-879, 83-101.	0.9	2
196	On the Existence of Pseudorandom Generators. Lecture Notes in Computer Science, 1990, , 146-162.	1.3	2
197	On the Number of Close-and-Equal Pairs of Bits in a String (with Implications on the Security of RSAâ€™s) Tj ETQq1 1 0.784314 rgBT		2
198	On Security Preserving Reductions â€“ Revised Terminology. Lecture Notes in Computer Science, 2011, , 540-546.	1.3	2

#	Article	IF	Citations
199	A taxonomy of proof systems (part 1). ACM SIGACT News, 1993, 24, 2-13.	0.1	2
200	Probabilistic Proof Systems: A Primer. Foundations and Trends in Theoretical Computer Science, 2008, 3, 1-91.	0.3	2
201	Concurrent Zero-Knowledge with Timing, Revisited. Lecture Notes in Computer Science, 2006, , 27-87.	1.3	2
202	From Logarithmic Advice to Single-Bit Advice. Lecture Notes in Computer Science, 2011, , 109-113.	1.3	2
203	Constant-Round Interactive Proof Systems for AC0[2] and NC1. Lecture Notes in Computer Science, 2020, , 326-351.	1.3	2
204	Proofs that Release Minimum Knowledge. , 1986, , 639-650.		1
205	The future of computational complexity theory: part I. ACM SIGACT News, 1996, 27, 6-12.	0.1	1
206	On struggle and competition in scientic fields. ACM SIGACT News, 2012, 43, 43-60.	0.1	1
207	Proofs of proximity for context-free languages and read-once branching programs. Information and Computation, 2018, 261, 175-201.	0.7	1
208	Pseudorandomness. Lecture Notes in Computer Science, 2000, , 687-704.	1.3	1
209	Algorithmic Aspects of Property Testing in the Dense Graphs Model. Lecture Notes in Computer Science, 2009, , 520-533.	1.3	1
210	Hierarchy Theorems for Property Testing. Lecture Notes in Computer Science, 2010, , 289-294.	1.3	1
211	Contemplations on Testing Graph Properties. Lecture Notes in Computer Science, 2011, , 547-554.	1.3	1
212	Average Case Complexity, Revisited. Lecture Notes in Computer Science, 2011, , 422-450.	1.3	1
213	Another Motivation for Reducing the Randomness Complexity of Algorithms. Lecture Notes in Computer Science, 2011, , 555-560.	1.3	1
214	Flexible Models for Testing Graph Properties. Lecture Notes in Computer Science, 2020, , 352-362.	1.3	1
215	On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions. Lecture Notes in Computer Science, 2020, , 41-86.	1.3	1
216	Two Comments on Targeted Canonical Derandomizers. Lecture Notes in Computer Science, 2020, , 24-35.	1.3	1

#	Article	IF	Citations
217	On the number of monochromatic close pairs of beads in a rosary. Discrete Mathematics, 1990, 80, 59-68.	0.7	0
218	Critique of some trends in the TCS community in light of two controversies. ACM SIGACT News, 1992, 23, 44-46.	0.1	0
219	Special Issue on Randomness and Complexity. SIAM Journal on Computing, 2006, 36, ix-xi.	1.0	0
220	Preface to the Special Issue from Randomâ€™06. Computational Complexity, 2008, 17, 1-2.	0.3	0
221	Complexity Theory. Oberwolfach Reports, 2010, 6, 2787-2850.	0.0	0
222	A theory of goal-oriented communication. , 2011, , .		0
223	Special issue from RANDOMâ€™09: Editorsâ€™ Foreword. Computational Complexity, 2012, 21, 1-1.	0.3	0
224	Estimating Simple Graph Parameters in Sublinear Time. , 2016, , 650-653.		0
225	Special Issue on the 10th Theory of Cryptography Conference: Editorâ€™s Foreword. Computational Complexity, 2016, 25, 563-565.	0.3	0
226	On the impact of cryptography on complexity theory. , 2019, , .		0
227	On our duties as scientists. ACM SIGACT News, 2009, 40, 53-59.	0.1	0
228	The Program of the Mini-Workshop. Lecture Notes in Computer Science, 2010, , 6-12.	1.3	0
229	On the Circuit Complexity of Perfect Hashing. Lecture Notes in Computer Science, 2011, , 26-29.	1.3	0
230	The GGM Construction Does NOT Yield Correlation Intractable Function Ensembles. Lecture Notes in Computer Science, 2011, , 98-108.	1.3	0
231	A taxonomy of proof systems (part 2). ACM SIGACT News, 1994, 25, 22-30.	0.1	0
232	Estimating Simple Graph Parameters in Sublinear Time. , 2015, , 1-5.		0
233	Testing Bipartiteness of Graphs in Sublinear Time. , 2015, , 1-5.		0
234	Testing Bipartiteness in the Dense-Graph Model. , 2016, , 2212-2216.		0

#	Article	IF	Citations
235	Testing Bipartiteness of Graphs in Sublinear Time. , 2016, , 2216-2219.		0
236	Pseudo-mixing Time of Random Walks. Lecture Notes in Computer Science, 2020, , 363-373.	1.3	0
237	The Subgraph Testing Model. ACM Transactions on Computation Theory, 2020, 12, 1-32.	0.7	0
238	On the Effect of the Proximity Parameter on Property Testers. Lecture Notes in Computer Science, 2020, , 36-40.	1.3	0
239	On the Relation Between the Relative Earth Mover Distance and the Variation Distance (an Exposition). Lecture Notes in Computer Science, 2020, , 141-151.	1.3	0
240	On Constant-Depth Canonical Boolean Circuits for Computing Multilinear Functions. Lecture Notes in Computer Science, 2020, , 306-325.	1.3	0
241	On Emulating Interactive Proofs with Public Coins. Lecture Notes in Computer Science, 2020, , 178-198.	1.3	0
242	Bridging a Small Gap in the Gap Amplification of Assignment Testers. Lecture Notes in Computer Science, 2020, , 9-16.	1.3	0
243	On Concurrent Identification Protocols (Extended Abstract). , 1984, , 387-396.		0
244	Improved bounds on the AN-complexity of $$O(1)$$-linear functions. Computational Complexity, 2022, 31, .	0.3	0