Hardness vs randomness

Journal of Computer and System Sciences

49, 149-167

DOI: 10.1016/s0022-0000(05)80043-1

Citation Report

#	Article	IF	Citations
1	On Tally Relativizations of BP-Complexity Classes. SIAM Journal on Computing, 1989, 18, 449-462.	1.0	17
2	Worlds to die for. ACM SIGACT News, 1995, 26, 5-15.	0.1	10
3	Hard-core distributions for somewhat hard problems. , 0, , .		115
4	Computing Solutions Uniquely Collapses the Polynomial Hierarchy. SIAM Journal on Computing, 1996, 25, 697-708.	1.0	53
5	Index sets and presentations of complexity classes. Theoretical Computer Science, 1996, 161, 263-287.	0.9	2
6	Circuit complexity before the dawn of the new millennium. Lecture Notes in Computer Science, 1996, , 1-18.	1.3	18
7	P = BPP if E requires exponential circuits. , 1997, , .		359
8	Weak random sources, hitting sets, and BPP simulations. , 0, , .		13
9	On resource-bounded measure and pseudorandomness. Lecture Notes in Computer Science, 1997, , 235-249.	1.3	26
10	Making nondeterminism unambiguous. , 0, , .		14
11	On operators of higher types. , 0, , .		2
12	Efficient constructions of Hitting Sets for systems of linear functions. Lecture Notes in Computer Science, 1997, , 387-398.	1.3	2
13	Observations on measure and lowness for Î” 2 P. Theory of Computing Systems, 1997, 30, 429-442.	1.1	10
14	Observations on Measure and Lowness for Î” P_2. Theory of Computing Systems, 1997, 30, 429-442.	1.1	7
15	Optimal bounds for the approximation of boolean functions and some applications. Theoretical Computer Science, 1997, 180, 243-268.	0.9	6
16	Probabilistic Type-2 Operators and "Almost"-Classes. Computational Complexity, 1998, 7, 265-289.	0.3	1
17	Resource bounded measure and learnability. , 0, , .		1
18	On the resource bounded measure of P/poly. , 0, , .		1

#	Article	IF	Citations
19	Randomness vs. time: de-randomization under a uniform assumption. , 0, , .		33
20	Equivalence Problems and Lower Bounds for Branching Programs. , 1998, , 115-122.		0
21	A new general derandomization method. Journal of the ACM, 1998, 45, 179-213.	2.2	36
22	Uniformly hard languages. , 0, , .		0
23	Isolation, matching, and counting. , 0, , .		4
24	Hard sets are hard to find. , 0, , .		2
25	A generalization of resource-bounded measure, with an application (Extended abstract). Lecture Notes in Computer Science, 1998, , 161-171.	1.3	7
26	Do probabilistic algorithms outperform deterministic ones?. Lecture Notes in Computer Science, 1998, , 212-214.	1.3	1
27	Extracting all the randomness and reducing the error in Trevisan's extractors. , 1999, , .		66
28	Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. , 1999, , .		46
29	Pseudorandom generators without the XOR Lemma (extended abstract). , 1999, , .		37
30	Hardness and hierarchy theorems for probabilistic quasi-polynomial time. , 1999, , .		9
31	Construction of extractors using pseudo-random generators (extended abstract). , 1999, , .		45
32	Worst-case hardness suffices for derandomization: a new method for hardness-randomness trade-offs. Theoretical Computer Science, 1999, 221, 3-18.	0.9	6
33	Relativized worlds with an infinite hierarchy. Information Processing Letters, 1999, 69, 309-313.	0.6	15
34	Synthesizers and Their Application to the Parallel Construction of Pseudo-Random Functions. Journal of Computer and System Sciences, 1999, 58, 336-375.	1.2	88
35	Isolation, Matching, and Counting Uniform and Nonuniform Upper Bounds. Journal of Computer and System Sciences, 1999, 59, 164-181.	1.2	49
36	Hard Sets Are Hard to Find. Journal of Computer and System Sciences, 1999, 59, 327-345.	1.2	11

#	Article	IF	Citations
37	De-randomizing BPP: the state of the art. , 0, , .		2
38	Pseudorandom generators without the XOR lemma. , 0, , .		33
39	Boosting and hard-core sets. , 0, , .		20
40	Weak Random Sources, Hitting Sets, and BPP Simulations. SIAM Journal on Computing, 1999, 28, 2103-2116.	1.0	33
41	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, 1999, , .	0.6	130
42	Derandomizing Arthur-Merlin games using hitting sets. , 0, , .		33
43	Immunity and Simplicity for Exact Counting and Other Counting Classes. RAIRO - Theoretical Informatics and Applications, 1999, 33, 159-176.	0.5	9
44	Resource-Bounded Measure and Learnability. Theory of Computing Systems, 2000, 33, 151-170.	1.1	6
45	List decoding. ACM SIGACT News, 2000, 31, 16-27.	0.1	83
46	Are bitvectors optimal?. , 2000, , .		27
47	On transformation of interactive proofs that preserve the prover's complexity. , 2000, , .		5
48	Towards uniform AC/sup 0/-isomorphisms. , 0, , .		0
49	In search of an easy witness: exponential time vs. probabilistic polynomial time. , 0, , .		1
51	Making Nondeterminism Unambiguous. SIAM Journal on Computing, 2000, 29, 1118-1131.	1.0	60
52	A Generalization of Resource-Bounded Measure, with Application to the BPP vs. EXP Problem. SIAM Journal on Computing, 2000, 30, 576-601.	1.0	17
53	Circuit minimization problem. , 2000, , .		79
54	STACS 2000. Lecture Notes in Computer Science, 2000, , .	1.3	1
55	Easiness assumptions and hardness tests: trading time for zero error. , 0, , .		12

#	Article	IF	Citations
56	Pseudorandom generators in propositional proof complexity. , 0, , .		19
57	Simple analysis of graph tests for linearity and PCP. , 0, , .		1
58	Computational depth. , 0, , .		1
59	Extracting randomness from samplable distributions. , 0, , .		88
60	The quantum complexity of set membership. , 0, , .		1
61	Derandomizing Arthur--Merlin games under uniform assumptions. Computational Complexity, 2001, 10, 247-259.	0.3	18
62	On pseudorandomness and resource-bounded measure. Theoretical Computer Science, 2001, 255, 205-221.	0.9	24
63	Pseudorandom Generators without the XOR Lemma. Journal of Computer and System Sciences, 2001, 62, 236-266.	1.2	243
64	Easiness Assumptions and Hardness Tests: Trading Time for Zero Error. Journal of Computer and System Sciences, 2001, 63, 236-252.	1.2	46
65	Randomness vs Time: Derandomization under a Uniform Assumption. Journal of Computer and System Sciences, 2001, 63, 672-688.	1.2	60
66	Extractors from Reed-Muller codes. , 2001, , .		36
67	Simple extractors for all min-entropies and a new pseudo-random generator. , 2001, , .		57
68	Extractors and pseudorandom generators. Journal of the ACM, 2001, 48, 860-879.	2.2	220
69	Loss-less condensers, unbalanced expanders, and extractors. , 2001, , .		80
70	Pseudorandomness and average-case complexity via uniform reductions. , 0, , .		24
71	Quality Control in Manufacturing Oligo Arrays: A Combinatorial Design Approach. Journal of Computational Biology, 2002, 9, 1-22.	1.6	24
72	Algorithmic derandomization via complexity theory. , 2002, , .		41
73	Pseudo-random generators for all hardnesses. , 2002, , .		38

#	Article	IF	Citations
74	Pseudo-random generators and structure of complete degrees. , 0, , .		14
75	Power from random strings. , 0, , .		11
76	Are Bitvectors Optimal?. SIAM Journal on Computing, 2002, 31, 1723-1744.	1.0	73
77	Graph Nonisomorphism Has Subexponential Size Proofs Unless the Polynomial-Time Hierarchy Collapses. SIAM Journal on Computing, 2002, 31, 1501-1526.	1.0	142
78	Extracting all the Randomness and Reducing the Error in Trevisan's Extractors. Journal of Computer and System Sciences, 2002, 65, 97-128.	1.2	80
79	New Lowness Results for ZPPNP and Other Complexity Classes. Journal of Computer and System Sciences, 2002, 65, 257-277.	1.2	10
80	The Quantum Complexity of Set Membership. Algorithmica, 2002, 34, 462-479.	1.3	2
81	Constructing set systems with prescribed intersection sizes. Journal of Algorithms, 2002, 44, 321-337.	0.9	23
82	In search of an easy witness: exponential time vs. probabilistic polynomial time. Journal of Computer and System Sciences, 2002, 65, 672-694.	1.2	156
83	Boosting and Hard-Core Set Construction. Machine Learning, 2003, 51, 217-238.	5.4	38
84	Uniform hardness versus randomness tradeoffs for Arthur-Merlin games. Computational Complexity, 2003, 12, 85.	0.3	32
85	Pseudo-random generators for all hardnesses. Journal of Computer and System Sciences, 2003, 67, 419-440.	1.2	64
86	Uniformly hard languages. Theoretical Computer Science, 2003, 298, 303-315.	0.9	10
87	NL-printable sets and Nondeterministic Kolmogorov Complexity. Electronic Notes in Theoretical Computer Science, 2003, 84, 1-15.	0.9	2
88	Simple analysis of graph tests for linearity and PCP. Random Structures and Algorithms, 2003, 22, 139-160.	1.1	61
89	On the distribution of the number of roots of polynomials and explicit weak designs. Random Structures and Algorithms, 2003, 23, 235-263.	1.1	20
90	Derandomization and distinguishing complexity. , 0, , .		6
91	Uniform hardness vs. randomness tradeoffs for Arthur-Merlin games. , 0, , .		8

#	Article	IF	Citations
92	Holographic proofs and derandomization. , 0, , .		0
93	On derandomizing tests for certain polynomial identities. , 0, , .		6
94	Quantum certificate complexity. , 0, , .		7
95	Hardness vs. randomness within alternating time. , 0, , .		6
96	Computing and Combinatorics. Lecture Notes in Computer Science, 2003, , .	1.3	1
97	Cell-probe lower bounds for the partial match problem. , 2003, , .		15
98	Sampling lower bounds via information theory. , 2003, , .		24
99	Derandomizing polynomial identity tests means proving circuit lower bounds. , 2003, , .		44
100	Solvable group isomorphism is (almost) in NP â^© coNP. , 0, , .		2
101	Small spans in scaled dimension. , 0, , .		4
102	Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. Journal of Symbolic Logic, 2004, 69, 265-286.	0.5	54
103	A Note on Approximate Counting for k-DNF. Lecture Notes in Computer Science, 2004, , 417-425.	1.3	26
104	Using nondeterminism to amplify hardness. , 2004, , .		16
105	Extractor Codes. IEEE Transactions on Information Theory, 2004, 50, 3015-3025.	2.4	43
106	Average-case intractability vs. worst-case intractability. Information and Computation, 2004, 190, 1-17.	0.7	4
107	Minimum ?-equivalent Circuit Size Problem. Journal of Combinatorial Optimization, 2004, 8, 495-502.	1.3	1
108	Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. Computational Complexity, 2004, 13, 1-46.	0.3	260
109	The size of SPP. Theoretical Computer Science, 2004, 320, 495-503.	0.9	5

#	Article	IF	Citations
110	Hardness amplification within NP. Journal of Computer and System Sciences, 2004, 69, 68-94.	1.2	40
111	Cell-probe lower bounds for the partial match problem. Journal of Computer and System Sciences, 2004, 69, 435-447.	1.2	15
112	Dual weak pigeonhole principle, Boolean complexity, and derandomization. Annals of Pure and Applied Logic, 2004, 129, 1-37.	0.5	76
113	Quantum Arthur-Merlin games. , 0, , .		3
114	Language compression and pseudorandom generators. , 0, , .		1
115	Properties of NP-complete sets. , 0, , .		1
116	Small Spans in Scaled Dimension. SIAM Journal on Computing, 2004, 34, 170-194.	1.0	11
117	Pseudorandom Generators in Propositional Proof Complexity. SIAM Journal on Computing, 2004, 34, 67-88.	1.0	71
118	On Proving Circuit Lower Bounds against the Polynomial-Time Hierarchy. SIAM Journal on Computing, 2004, 33, 984-1009.	1.0	7
119	Deterministic Hypergraph Coloring and Its Applications. SIAM Journal on Discrete Mathematics, 2004, 18, 320-331.	0.8	1
120	RECENT DEVELOPMENTS IN EXPLICIT CONSTRUCTIONS OF EXTRACTORS. , 2004, , 189-228.		60
122	Resource bounded symmetry of information revisited. Theoretical Computer Science, 2005, 345, 386-405.	0.9	11
123	The complexity of constructing pseudorandom generators from hard functions. Computational Complexity, 2005, 13, 147-188.	0.3	63
124	Quantum Arthurâ€“Merlin games. Computational Complexity, 2005, 14, 122-152.	0.3	138
125	Derandomizing Arthurâ€“Merlin Games using Hitting Sets. Computational Complexity, 2005, 14, 256-279.	0.3	41
126	Compression of Samplable Sources. Computational Complexity, 2005, 14, 186-227.	0.3	10
127	Language compression and pseudorandom generators. Computational Complexity, 2005, 14, 228-255.	0.3	7
128	Pseudorandom generators for low degree polynomials. , 2005, , .		22

#	Article	IF	Citations
129	Simple extractors for all min-entropies and a new pseudorandom generator. Journal of the ACM, 2005, 52, 172-216.	2.2	101
130	List Decoding of Error-Correcting Codes. Lecture Notes in Computer Science, 2005, , .	1.3	64
131	NONDETERMINISTIC CIRCUIT MINIMIZATION PROBLEM AND DERANDOMIZING ARTHUR-MERLIN GAMES. International Journal of Foundations of Computer Science, 2005, 16, 1297-1308.	1.1	4
132	Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques. Lecture Notes in Computer Science, 2005, , .	1.3	7
133	Holographic Proofs and Derandomization. SIAM Journal on Computing, 2005, 35, 59-90.	1.0	14
134	Pseudorandomness for Approximate Counting and Sampling. , 0, , .		9
135	On Constructing Parallel Pseudorandom Generators from One-Way Functions. , 0, , .		30
136	On the Complexity of Hardness Amplification. , 0, , .		2
137	NP with Small Advice. , 0, , .		6
138	Pseudorandom Bits for Constant Depth Circuits with Few Arbitrary Symmetric Gates. , 0, , .		3
139	Exposure-Resilient Extractors. , 0, , .		6
141	Making Hard Problems Harder. , 0, , .		5
142	Approximately List-Decoding Direct Product Codes and Uniform Hardness Amplification. , 2006, , .		21
143	Power from Random Strings. SIAM Journal on Computing, 2006, 35, 1467-1493.	1.0	77
144	Using Nondeterminism to Amplify Hardness. SIAM Journal on Computing, 2006, 35, 903-931.	1.0	38
145	Properties of NPâ€Complete Sets. SIAM Journal on Computing, 2006, 36, 516-542.	1.0	6
146	Extractors from Reedâ€"Muller codes. Journal of Computer and System Sciences, 2006, 72, 786-812.	1.2	22
147	NL-printable sets and nondeterministic Kolmogorov complexity. Theoretical Computer Science, 2006, 355, 127-138.	0.9	5

#	Article	IF	Citations
148	On zero error algorithms having oracle access to one query. Journal of Combinatorial Optimization, 2006, 11, 189-202.	1.3	8
149	Random Access to Advice Strings and Collapsing Results. Algorithmica, 2006, 46, 43-57.	1.3	0
150	Reducing The Seed Length In The Nisan-Wigderson Generator*. Combinatorica, 2006, 26, 647-681.	1.2	13
151	Pseudorandomness for Approximate Counting and Sampling. Computational Complexity, 2006, 15, 298-341.	0.3	32
152	Computational depth: Concept and applications. Theoretical Computer Science, 2006, 354, 391-404.	0.9	41
153	Hardness of approximate two-level logic minimization and PAC learning with membership queries. , 2006, , .		11
154	Can every randomized algorithm be derandomized?. , 2006, , .		4
155	On the randomness complexity of efficient sampling. , 2006, , .		37
156	How to Get More Mileage from Randomness Extractors. , 0, , .		15
157	List Decoding in Average-Case Complexity and Pseudorandomness. , 0, , .		8
158	Circuit lower bounds for Merlin-Arthur classes. , 2007, , .		13
159	Low-end uniform hardness vs. randomness tradeoffs for AM. , 2007, , .		9
160	Derandomization in Cryptography. SIAM Journal on Computing, 2007, 37, 380-400.	1.0	47
161	Approximate counting in bounded arithmetic. Journal of Symbolic Logic, 2007, 72, 959-993.	0.5	50
162	The unified theory of pseudorandomness. ACM SIGACT News, 2007, 38, 39-54.	0.1	18
163	Pseudorandom Bits for Constantâ€Depth Circuits with Few Arbitrary Symmetric Gates. SIAM Journal on Computing, 2007, 36, 1387-1403.	1.0	43
164	Low-Depth Witnesses are Easy to Find. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	2
165	Bounded Queries and the NP Machine Hypothesis. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	1

#	Article	IF	Citations
166	Norms, XOR Lemmas, and Lower Bounds for GF(2) Polynomials and Multiparty Protocols. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	29
167	S-T Connectivity on Digraphs with a Known Stationary Distribution. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	25
168	On Derandomizing Probabilistic Sublinear-Time Algorithms. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	5
169	Upward separations and weaker hypotheses in resource-bounded measure. Theoretical Computer Science, 2007, 389, 162-171.	0.9	3
170	Pseudorandomness and Average-Case Complexity Via Uniform Reductions. Computational Complexity, 2007, 16, 331-364.	0.3	61
171	Quantum certificate complexity. Journal of Computer and System Sciences, 2008, 74, 313-322.	1.2	12
172	Exposure-Resilient Extractors and the Derandomization of Probabilistic Sublinear Time. Computational Complexity, 2008, 17, 220-253.	0.3	8
173	Dimension Characterizations of Complexity Classes. Computational Complexity, 2008, 17, 459-474.	0.3	1
174	Relations between Average-Case and Worst-Case Complexity. Theory of Computing Systems, 2008, 42, 596-607.	1.1	0
175	How to get more mileage from randomness extractors. Random Structures and Algorithms, 2008, 33, 157-186.	1.1	15
176	On the Complexity of Hardness Amplification. IEEE Transactions on Information Theory, 2008, 54, 4575-4586.	2.4	8
177	Average-case Complexity. , 2008, , .		0
178	Arithmetic Circuits: A Chasm at Depth Four. , 2008, , .		105
179	Hardness amplification proofs require majority. , 2008, , .		12
180	Hardness-randomness tradeoffs for bounded depth arithmetic circuits. , 2008, , .		4
182	Complexity Theory. Oberwolfach Reports, 2010, 6, 2787-2850.	0.0	0
183	Are PCPs Inherent in Efficient Arguments?. , 2009, , .		6
184	Weak Derandomization of Weak Algorithms: Explicit Versions of Yao's Lemma. , 2009, , .		6

#	Article	IF	Citations
185	Chapter 4 A Status Report on the P Versus NP Question. Advances in Computers, 2009, 77, 117-147.	1.6	2
186	Short seed extractors against quantum storage. , 2009, , .		11
187	Reconstructive Dispersers and Hitting Set Generators. Algorithmica, 2009, 55, 134-156.	1.3	2
188	Comparing Notions of Computational Entropy. Theory of Computing Systems, 2009, 45, 944-962.	1.1	4
189	Hardness of approximate two-level logic minimization and PAC learning with membership queries. Journal of Computer and System Sciences, 2009, 75, 13-26.	1.2	24
191	Fixed-Polynomial Size Circuit Bounds. , 2009, , .		10
192	2-Source Extractors under Computational Assumptions and Cryptography with Defective Randomness. , 2009, , .		17
193	Worst-Case Running Times for Average-Case Algorithms. , 2009, , .		11
194	Approximate List-Decoding of Direct Product Codes and Uniform Hardness Amplification. SIAM Journal on Computing, 2009, 39, 564-605.	1.0	10
195	Low-End Uniform Hardness versus Randomness Tradeoffs for AM. SIAM Journal on Computing, 2009, 39, 1006-1037.	1.0	8
196	Circuit Lower Bounds for Merlinâ€“Arthur Classes. SIAM Journal on Computing, 2009, 39, 1038-1061.	1.0	29
197	Classifying Problems on Linear Congruences and Abelian Permutation Groups Using Logspace Counting Classes. Computational Complexity, 2010, 19, 57-98.	0.3	5
198	Are PCPs Inherent in Efficient Arguments?. Computational Complexity, 2010, 19, 265-304.	0.3	11
199	Underapproximation for model-checking based on universal circuits. Information and Computation, 2010, 208, 315-326.	0.7	0
200	The Gelfand widths of<mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.gif" display="inline" overflow="scroll"><mml:msub><mml:mrow><mml:mi>â„“</mml:mi></mml:mrow><mml:mrow><mml:mi>p</mml:mi></mml:mrow></m for<mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si2.gif" display="inline" overflow="scroll"><mml:mn>0</mml:mn><mml:mo>&lt;</mml:mo><mml:mi>p</mml:mi><mml:mo>â‰</mml:mo><mml:mn>1</mml:m Journal of Complexity, 2010, 26, 629-640.	1.3	76
201	Simple extractors via constructions of cryptographic pseudo-random generators. Theoretical Computer Science, 2010, 411, 1236-1250.	0.9	2
203	Hardness-Randomness Tradeoffs for Bounded Depth Arithmetic Circuits. SIAM Journal on Computing, 2010, 39, 1279-1293.	1.0	39
204	Simple Affine Extractors Using Dimension Expansion. , 2010, , .		12

#	Article	IF	Citations
205	Near-optimal extractors against quantum storage. , 2010, , .		9
206	ON THE HARDNESS AGAINST CONSTANT-DEPTH LINEAR-SIZE CIRCUITS. Discrete Mathematics, Algorithms and Applications, 2010, 02, 515-526.	0.6	0
207	Hardness Amplification Proofs Require Majority. SIAM Journal on Computing, 2010, 39, 3122-3154.	1.0	49
208	On the Power of Randomized Reductions and the Checkability of SAT. , 2010, , .		14
209	The Complexity of Distributions. , 2010, , .		11
210	Codes for Computationally Simple Channels: Explicit Constructions with Optimal Rate. , 2010, , .		46
211	Pseudorandom Generators for Combinatorial Checkerboards. , 2011, , .		2
212	Pseudorandomness for Permutation and Regular Branching Programs. , 2011, , .		23
213	Symmetry of Information and Bounds on Nonuniform Randomness Extraction via Kolmogorov Extractors. , 2011, , .		7
214	Short Seed Extractors against Quantum Storage. SIAM Journal on Computing, 2011, 40, 664-677.	1.0	2
215	Random Walks and Rapid Mixing. , 2011, , 563-650.		1
216	Extracting Kolmogorov complexity with applications to dimension zero-one laws. Information and Computation, 2011, 209, 627-636.	0.7	9
217	Weak Derandomization of Weak Algorithms: Explicit Versions of Yaoâ€™s Lemma. Computational Complexity, 2011, 20, 87-143.	0.3	10
218	Derandomizing Arthur-Merlin Games and Approximate Counting Implies Exponential-Size Lower Bounds. Computational Complexity, 2011, 20, 329-366.	0.3	9
219	Arthur and Merlin as Oracles. Computational Complexity, 2011, 20, 505-558.	0.3	3
220	Variations on Muchnikâ€™s Conditional Complexity Theorem. Theory of Computing Systems, 2011, 49, 227-245.	1.1	12
221	The pervasive reach of resource-bounded Kolmogorov complexity in computational complexity theory. Journal of Computer and System Sciences, 2011, 77, 14-40.	1.2	26
222	Nisan-Wigderson generators in proof systems with forms of interpolation. Mathematical Logic Quarterly, 2011, 57, 379-383.	0.2	29

#	Article	IF	Citations
223	The isomorphism conjecture for constant depth reductions. Journal of Computer and System Sciences, 2011, 77, 3-13.	1.2	9
224	S-T connectivity on digraphs with a known stationary distribution. ACM Transactions on Algorithms, 2011, 7, 1-21.	1.0	8
225	Repeated matching pennies with limited randomness. , 2011, , .		4
226	Formalizing Randomized Matching Algorithms. , 2011, , .		1
227	Solvable Group Isomorphism Is (Almost) in NP â^© coNP. ACM Transactions on Computation Theory, 2011, 2, 1-22.	0.7	7
228	ON THE PROOF COMPLEXITY OF THE NISANâ€"WIGDERSON GENERATOR BASED ON A HARD <font>NP</font> â^© <font>coNP</font> FUNCTION. Journal of Mathematical Logic, 2011, 11, 11-27.	0.6	36
229	On P vs. NP and geometric complexity theory. Journal of the ACM, 2011, 58, 1-26.	2.2	34
230	Pseudorandomness and derandomization. Xrds, 2012, 18, 27-31.	0.3	2
231	Design extractors, non-malleable condensers and privacy amplification. , 2012, , .		20
232	On beating the hybrid argument. , 2012, , .		3
233	Marginal hitting sets imply super-polynomial lower bounds for permanent. , 2012, , .		6
234	Tight bounds for monotone switching networks via fourier analysis. , 2012, , .		4
235	Geometric Complexity Theory V: Equivalence between Blackbox Derandomization of Polynomial Identity Testing and Derandomization of Noether's Normalization Lemma. , 2012, , .		29
236	A Satisfiability Algorithm and Average-Case Hardness for Formulas over the Full Binary Basis. , 2012, , .		13
237	Uniform derandomization from pathetic lower bounds. Philosophical Transactions Series A, Mathematical, Physical, and Engineering Sciences, 2012, 370, 3512-3535.	3.4	1
238	Trevisan's Extractor in the Presence of Quantum Side Information. SIAM Journal on Computing, 2012, 41, 915-940.	1.0	67
239	The Complexity of Distributions. SIAM Journal on Computing, 2012, 41, 191-218.	1.0	25
240	Low-Depth Witnesses are Easy to Find. Computational Complexity, 2012, 21, 479-497.	0.3	2

#	Article	IF	Citations
241	DNF Sparsification and a Faster Deterministic Counting Algorithm. , 2012, , .		5
242	Nondeterministic Circuit Lower Bounds from Mildly De-randomizing Arthur-Merlin Games. , 2012, , .		5
243	Pseudorandom Generators for Read-Once ACC^0. , 2012, , .		0
244	Pseudorandomness from Shrinkage. , 2012, , .		32
245	Pseudorandomness. Foundations and Trends in Theoretical Computer Science, 2012, 7, 1-336.	0.3	160
246	Towards a tight hardnessâ€“randomness connection between permanent and arithmetic circuit identity testing. Information Processing Letters, 2012, 112, 969-975.	0.6	0
247	Pseudorandom Generators, Typically-Correct Derandomization, and Circuit Lower Bounds. Computational Complexity, 2012, 21, 3-61.	0.3	18
248	Random low-degree polynomials are hard to approximate. Computational Complexity, 2012, 21, 63-81.	0.3	6
249	Collapsing and Separating Completeness Notions Under Average-Case and Worst-Case Hypotheses. Theory of Computing Systems, 2012, 51, 248-265.	1.1	3
250	The Complexity of Explicit Constructions. Theory of Computing Systems, 2012, 51, 297-312.	1.1	3
251	On derandomization and average-case complexity of monotone functions. Theoretical Computer Science, 2012, 434, 35-44.	0.9	3
252	Logical Foundations of Mathematics and Computational Complexity. Springer Monographs in Mathematics, 2013, , .	0.2	37
253	Theory and Applications of Models of Computation. Lecture Notes in Computer Science, 2013, , .	1.3	0
254	Space-Efficient Data Structures, Streams, and Algorithms. Lecture Notes in Computer Science, 2013, , .	1.3	3
255	Pseudorandom generators for CC0[p] and the Fourier spectrum of low-degree polynomials over finite fields. Computational Complexity, 2013, 22, 679-725.	0.3	3
256	Pseudorandom generators for combinatorial checkerboards. Computational Complexity, 2013, 22, 727-769.	0.3	4
257	DNF sparsification and a faster deterministic counting algorithm. Computational Complexity, 2013, 22, 275-310.	0.3	26
258	The complexity of inverting explicit Goldreichâ€™s function by DPLL algorithms. Journal of Mathematical Sciences, 2013, 188, 47-58.	0.4	2

#	Article	IF	Citations
259	Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. Physical Review A, 2013, 87, .	2.5	153
260	The Complexity of Computations. Springer Monographs in Mathematics, 2013, , 365-493.	0.2	13
261	A satisfiability algorithm and average-case hardness for formulas over the full binary basis. Computational Complexity, 2013, 22, 245-274.	0.3	20
262	Limits on the computational power of random strings. Information and Computation, 2013, 222, 80-92.	0.7	13
263	Can theories be tested?. , 2013, , .		3
264	Natural proofs versus derandomization. , 2013, , .		16
265	Resource-based corruptions and the combinatorics of hidden diversity. , 2013, , .		8
266	Average-case lower bounds for formula size. , 2013, , .		19
267	Pseudorandom Generators with Long Stretch and Low Locality from Random Local One-Way Functions. SIAM Journal on Computing, 2013, 42, 2008-2037.	1.0	30
268	Nondeterministic Direct Product Reductions and the Success Probability of SAT Solvers. , 2013, , .		5
270	Turing and the development of computational complexity. , 0, , 299-328.		1
271	Timing in chemical reaction networks. , 2014, , .		26
272	On the computational complexity of finding hard tautologies. Bulletin of the London Mathematical Society, 2014, 46, 111-125.	0.8	30
273	Computational Complexity. Handbook of the History of Logic, 2014, 9, 495-521.	0.5	0
274	A super-polynomial lower bound for regular arithmetic formulas. , 2014, , .		34
275	On derandomizing algorithms that err extremely rarely. , 2014, , .		13
276	Pseudorandom generators with optimal seed length for non-boolean poly-size circuits. , 2014, , .		1
277	Nonuniform ACC Circuit Lower Bounds. Journal of the ACM, 2014, 61, 1-32.	2.2	80

#	Article	IF	Citations
278	Improving the Space-Bounded Version of Muchnikâ€™s Conditional Complexity Theorem via â€œNaiveâ€• Derandomization. Theory of Computing Systems, 2014, 55, 299-312.	1.1	4
279	Pseudo-Random Graphs and Bit Probe Schemes with One-Sided Error. Theory of Computing Systems, 2014, 55, 313-329.	1.1	1
280	Lower Bound on Average-Case Complexity of Inversion of Goldreichâ€™s Function by Drunken Backtracking Algorithms. Theory of Computing Systems, 2014, 54, 261-276.	1.1	3
281	Deterministic function computation with chemical reaction networks. Natural Computing, 2014, 13, 517-534.	3.0	88
282	Algorithms for Circuits and Circuits for Algorithms. , 2014, , .		7
283	Fourier Concentration from Shrinkage. , 2014, , .		3
284	Deterministic Approximate Counting for Juntas of Degree-2 Polynomial Threshold Functions. , 2014, , .		4
285	Classifying Problems into Complexity Classes. Advances in Computers, 2014, , 239-292.	1.6	5
286	Perspectives in Computational Complexity. , 2014, , .		3
287	Turing in Quantumland. , 0, , 70-89.		0
288	Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. Annals of Mathematics, 2015, 181, 415-472.	4.2	45
289	Unifying Known Lower Bounds via Geometric Complexity Theory. Computational Complexity, 2015, 24, 393-475.	0.3	17
290	Mining Circuit Lower Bound Proofs for Meta-Algorithms. Computational Complexity, 2015, 24, 333-392.	0.3	23
291	Complexity Theory Column 88. ACM SIGACT News, 2015, 46, 32-49.	0.1	8
292	On the existence of compactÎµ-approximated formulations for knapsack in the original space. Operations Research Letters, 2015, 43, 339-342.	0.7	3
293	Advice Lower Bounds for the Dense Model Theorem. ACM Transactions on Computation Theory, 2015, 7, 1-18.	0.7	1
294	On the Complexity of Constructing Pseudorandom Functions (Especially when They Donâ€™t Exist). Journal of Cryptology, 2015, 28, 509-532.	2.8	0
295	On Extracting Space-bounded Kolmogorov Complexity. Theory of Computing Systems, 2015, 56, 643-661.	1.1	0

#	Article	IF	Citations
296	Circuit lower bounds in bounded arithmetics. Annals of Pure and Applied Logic, 2015, 166, 29-45.	0.5	35
297	On Optimal Language Compression for Sets in PSPACE/poly. Theory of Computing Systems, 2015, 56, 581-590.	1.1	0
298	Natural Proofs versus Derandomization. SIAM Journal on Computing, 2016, 45, 497-529.	1.0	16
299	Incompressible Functions, Relative-Error Extractors, and the Power of Nondeterministic Reductions. Computational Complexity, 2016, 25, 349-418.	0.3	9
300	Pseudorandom generators against advised context-free languages. Theoretical Computer Science, 2016, 613, 1-27.	0.9	3
301	Geometric complexity theory V: Efficient algorithms for Noether normalization. Journal of the American Mathematical Society, 2016, 30, 225-309.	3.9	19
302	$$mathrm {3SUM}$$ 3 SUM , $$mathrm {3XOR}$$ 3 XOR , Triangles. Algorithmica, 2016, 74, 326-343.	1.3	10
303	Nondeterministic circuit lower bounds from mildly derandomizing Arthur-Merlin games. Computational Complexity, 2017, 26, 79-118.	0.3	2
304	Random walks on graphs and Monte Carlo methods. Mathematics and Computers in Simulation, 2017, 135, 86-94.	4.4	5
305	Negation-limited formulas. Theoretical Computer Science, 2017, 660, 75-85.	0.9	5
306	Completeness for First-Order Properties on Sparse Structures with Algorithmic Applications. , 2017, , .		5
307	Open Problems Column. ACM SIGACT News, 2017, 48, 38-38.	0.1	0
308	Quantum random number generators. Reviews of Modern Physics, 2017, 89, .	45.6	412
309	Dimension, pseudorandomness and extraction of pseudorandomness1. Computability, 2017, 6, 277-305.	0.3	0
310	Computer Science â€“ Theory and Applications. Lecture Notes in Computer Science, 2017, , .	1.3	0
311	Pseudorandom Generators with Optimal Seed Length for Non-Boolean Poly-Size Circuits. ACM Transactions on Computation Theory, 2017, 9, 1-26.	0.7	4
312	Unexpected power of low-depth arithmetic circuits. Communications of the ACM, 2017, 60, 93-100.	4.5	0
313	On Approximating the Eigenvalues of Stochastic Matrices in Probabilistic Logspace. Computational Complexity, 2017, 26, 393-420.	0.3	6

#	Article	IF	Citations
314	Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms. Chaos, Solitons and Fractals, 2017, 104, 371-377.	5.1	15
315	Bounds on Monotone Switching Networks for Directed Connectivity. Journal of the ACM, 2017, 64, 1-48.	2.2	2
316	Robust simulations and significant separations. Information and Computation, 2017, 256, 149-159.	0.7	5
317	On the limits of depth reduction at depth 3 over small finite fields. Information and Computation, 2017, 256, 35-44.	0.7	0
318	Lower Bounds for the Circuit Size of Partially Homogeneous Polynomials. Journal of Mathematical Sciences, 2017, 225, 639-657.	0.4	0
319	A Generic Approach to Constructing and Proving Verifiable Random Functions. Lecture Notes in Computer Science, 2017, , 537-566.	1.3	36
320	Fourier Concentration from Shrinkage. Computational Complexity, 2017, 26, 275-321.	0.3	2
322	Deterministic Search for CNF Satisfying Assignments in Almost Polynomial Time. , 2017, , .		2
323	Targeted pseudorandom generators, simulation advice generators, and derandomizing logspace. , 2017, , .		1
324	Identity Testing and Lower Bounds for Read- <i>k</i> Oblivious Algebraic Branching Programs. ACM Transactions on Computation Theory, 2018, 10, 1-30.	0.7	5
325	Guest Column. ACM SIGACT News, 2018, 49, 55-65.	0.1	1
326	Time Bounded Incompressible Theorem Reversed. , 2018, , .		0
327	Non-Black-Box Worst-Case to Average-Case Reductions within NP. , 2018, , .		24
328	Hardness Magnification for Natural Problems. , 2018, , .		11
329	Bootstrapping variables in algebraic circuits. , 2018, , .		3
330	Quantified derandomization of linear threshold circuits. , 2018, , .		13
331	Hitting sets with near-optimal error for read-once branching programs. , 2018, , .		4
332	Pseudorandom Quantum States. Lecture Notes in Computer Science, 2018, , 126-152.	1.3	30

#	Article	IF	Citations
333	The Landscape of Communication Complexity Classes. Computational Complexity, 2018, 27, 245-304.	0.3	20
334	AC0âˆ˜MOD2 lower bounds for the Boolean Inner Product. Journal of Computer and System Sciences, 2018, 97, 45-59.	1.2	6
335	Minimum Circuit Size, Graph Isomorphism, and Related Problems. SIAM Journal on Computing, 2018, 47, 1339-1372.	1.0	14
336	On polynomial approximations to AC0. Random Structures and Algorithms, 2019, 54, 289-303.	1.1	6
337	Bootstrapping results for threshold circuits â€œjust beyondâ€•known lower bounds. , 2019, , .		16
338	Constant-Error Pseudorandomness Proofs from Hardness Require Majority. ACM Transactions on Computation Theory, 2019, 11, 1-11.	0.7	0
339	Proving that prBPPâ€¯=â€¯prP is as hard as proving that â€œalmost NPâ€•is not contained in P/poly. Information Processing Letters, 2019, 152, 105841.	0.6	4
340	Depth-4 Lower Bounds, Determinantal Complexity: A Unified Approach. Computational Complexity, 2019, 28, 545-572.	0.3	2
341	Testing graphs in vertex-distribution-free models. , 2019, , .		2
342	Fooling polytopes. , 2019, , .		7
343	A fixed-depth size-hierarchy theorem for AC <sup>0</sup> [âŠ•] via the coin problem. , 2019, , .		3
344	Completeness for First-order Properties on Sparse Structures with Algorithmic Applications. ACM Transactions on Algorithms, 2019, 15, 1-35.	1.0	8
345	Improved Bounds for Quantified Derandomization of Constant-Depth Circuits and Polynomials. Computational Complexity, 2019, 28, 259-343.	0.3	5
346	Bootstrapping variables in algebraic circuits. Proceedings of the National Academy of Sciences of the United States of America, 2019, 116, 8107-8118.	7.1	7
347	6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. Review of Scientific Instruments, 2019, 90, 043105.	1.3	56
349	Concepts and Problems. , 2019, , 11-38.		0
350	Examples of Upper Bounds and p-Simulations. , 2019, , 211-232.		0
351	Beyond EF via the || . . . || Translation. , 2019, , 233-260.		0

#	Article	IF	Citations
352	R and R-Like Proof Systems. , 2019, , 263-295.		0
353	Optimality. , 2019, , 456-471.		0
356	Open Problems Column. ACM SIGACT News, 2019, 50, 28-34.	0.1	1
357	Pseudorandomness from Shrinkage. Journal of the ACM, 2019, 66, 1-16.	2.2	8
359	Frege Systems. , 2019, , 39-63.		0
360	Sequent Calculus. , 2019, , 64-80.		0
361	Quantified Propositional Calculus. , 2019, , 81-92.		0
363	Algebraic and Geometric Proof Systems. , 2019, , 115-133.		0
364	Further Proof Systems. , 2019, , 134-162.		0
365	Basic Example of the Correspondence between Theories and Proof Systems. , 2019, , 165-184.		0
366	The Two Worlds of Bounded Arithmetic. , 2019, , 185-196.		0
367	Up to EF via the ã€ˆ. . .ã€‰ Translation. , 2019, , 197-210.		0
368	LKd+1/2 and Combinatorial Restrictions. , 2019, , 296-305.		0
369	Fd and Logical Restrictions. , 2019, , 306-336.		0
370	Algebraic and Geometric Proof Systems. , 2019, , 337-352.		0
371	Feasible Interpolation: A Framework. , 2019, , 353-383.		0
372	Feasible Interpolation: Applications. , 2019, , 384-410.		0
373	Hard Tautologies. , 2019, , 413-441.		0

#	Article	IF	Citations
374	Model Theory and Lower Bounds. , 2019, , 442-455.		0
375	The Nature of Proof Complexity. , 2019, , 472-480.		0
376	Non-deterministic Quasi-Polynomial Time is Average-Case Hard for ACC Circuits. , 2019, , .		16
377	Efficient Construction of Rigid Matrices Using an NP Oracle. , 2019, , .		16
378	Stoquastic PCP vs. Randomness. , 2019, , .		1
379	Derandomization from Algebraic Hardness: Treading the Borders. , 2019, , .		6
380	Why are Proof Complexity Lower Bounds Hard?. , 2019, , .		6
381	On Algorithmic Statistics for Space-bounded Algorithms. Theory of Computing Systems, 2019, 63, 833-848.	1.1	0
382	Entropy numbers of finite-dimensional embeddings. , 2020, 38, 319-336.		2
383	Feasibly constructive proofs of succinct weak circuit lower bounds. Annals of Pure and Applied Logic, 2020, 171, 102735.	0.5	9
384	Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. Physical Review A, 2020, 102, .	2.5	12
385	On the volume of unit balls of finite-dimensional Lorentz spaces. Journal of Approximation Theory, 2020, 255, 105407.	0.8	0
386	Pseudorandom Pseudo-distributions with Near-Optimal Error for Read-Once Branching Programs. SIAM Journal on Computing, 2020, 49, STOC18-242-STOC18-299.	1.0	4
387	Vacuum-based quantum random number generator using multi-mode coherent states. Quantum Information Processing, 2020, 19, 1.	2.2	4
388	Circuit Lower Bounds for Nondeterministic Quasi-polytime from a New Easy Witness Lemma. SIAM Journal on Computing, 2020, 49, STOC18-300-STOC18-322.	1.0	8
389	Explicit List-Decodable Codes with Optimal Rate for Computationally Bounded Channels. Computational Complexity, 2021, 30, 1.	0.3	4
390	On the Possibility of Basing Cryptography on $$mathsf{EXP}e mathsf{BPP}$$. Lecture Notes in Computer Science, 2021, , 11-40.	1.3	3
391	Cryptographic Pseudorandom Generators Can Make Cryptosystems Problematic. Lecture Notes in Computer Science, 2021, , 441-468.	1.3	1

#	Article	IF	Citations
392	Polynomial-Time Random Oracles and Separating Complexity Classes. ACM Transactions on Computation Theory, 2021, 13, 11-16.	0.7	0
393	Guest Column. ACM SIGACT News, 2021, 52, 47-69.	0.1	0
394	Targeted Pseudorandom Generators, Simulation Advice Generators, and Derandomizing Logspace. SIAM Journal on Computing, 2022, 51, STOC17-281-STOC17-304.	1.0	2
395	Simple and fast derandomization from very hard functions: eliminating randomness at almost no cost. , 2021, , .		7
396	Inverse-exponential correlation bounds and extremely rigid matrices from a new derandomized XOR lemma. , 2021, , .		5
397	Strong co-nondeterministic lower bounds for NP cannot be proved feasibly. , 2021, , .		4
399	A Secure Random Number Generator with Immunity and Propagation Characteristics for Cryptography Functions. Applied Sciences (Switzerland), 2021, 11, 8073.	2.5	1
400	Injective Trapdoor Functions via Derandomization: How Strong is Rudichâ€™s Black-Box Barrier?. Journal of Cryptology, 2021, 34, 1.	2.8	0
401	Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious-majority and free verification. Theoretical Computer Science, 2021, 886, 106-138.	0.9	5
402	A Fixed-Depth Size-Hierarchy Theorem for $mathrm{AC}^0[oplus]$ via the Coin Problem. SIAM Journal on Computing, 2021, 50, 1461-1499.	1.0	2
405	Lower Bounds for Circuits with Few Modular and Symmetric Gates. Lecture Notes in Computer Science, 2005, , 994-1005.	1.3	9
406	A Note on Zero Error Algorithms Having Oracle Access to One NP Query. Lecture Notes in Computer Science, 2005, , 339-348.	1.3	2
408	Hardness Amplification Via Space-Efficient Direct Products. Lecture Notes in Computer Science, 2006, , 556-568.	1.3	2
409	Extracting Kolmogorov Complexity with Applications to Dimension Zero-One Laws. Lecture Notes in Computer Science, 2006, , 335-345.	1.3	22
410	Dimension Characterizations of Complexity Classes. Lecture Notes in Computer Science, 2006, , 471-479.	1.3	2
411	On the Derandomization of Constant Depth Circuits. Lecture Notes in Computer Science, 2001, , 249-260.	1.3	11
412	Error-Correcting Codes and Pseudorandom Projections. Lecture Notes in Computer Science, 2001, , 7-9.	1.3	1
413	List Decoding: Algorithms and Applications. Lecture Notes in Computer Science, 2000, , 25-41.	1.3	12

#	Article	IF	Citations
414	When Worlds Collide: Derandomization, Lower Bounds, and Kolmogorov Complexity. Lecture Notes in Computer Science, 2001, , 1-15.	1.3	18
416	Hyper-encryption against Space-Bounded Adversaries from On-Line Strong Extractors. Lecture Notes in Computer Science, 2002, , 257-271.	1.3	25
417	Graph Isomorphism Is Low for ZPP(NP) and Other Lowness Results. Lecture Notes in Computer Science, 2000, , 431-442.	1.3	6
418	Small Pseudo-Random Sets Yield Hard Functions: New Tight Explicit Lower Bounds for Branching Programs. Lecture Notes in Computer Science, 1999, , 179-189.	1.3	11
419	Observations on measure and lowness for Î" 2 P. Lecture Notes in Computer Science, 1996, , 87-97.	1.3	5
420	Hitting sets derandomize BPP. Lecture Notes in Computer Science, 1996, , 357-368.	1.3	19
421	On type-2 probabilistic quantifiers. Lecture Notes in Computer Science, 1996, , 369-380.	1.3	6
423	Counting Complexity. , 1997, , 81-107.		36
424	A Taxonomy of Proof Systems. , 1997, , 109-134.		6
425	Measure One Results in Computational Complexity Theory. , 1997, , 285-312.		8
426	Non-Malleable Codes Against Bounded Polynomial Time Tampering. Lecture Notes in Computer Science, 2019, , 501-530.	1.3	9
427	A Note on Perfect Correctness by Derandomization. Lecture Notes in Computer Science, 2017, , 592-606.	1.3	17
429	Flavors of Compressive Sensing. Springer Proceedings in Mathematics and Statistics, 2017, , 61-104.	0.2	17
430	An Average-Case Lower Bound AgainstÂ $$mathsf {ACC}^0$$ ACC 0. Lecture Notes in Computer Science, 2018, , 317-330.	1.3	9
431	On the Hardness of Information-Theoretic Multiparty Computation. Lecture Notes in Computer Science, 2004, , 439-455.	1.3	29
432	Fooling Parity Tests with Parity Gates. Lecture Notes in Computer Science, 2004, , 381-392.	1.3	21
433	On Polynomially Time Bounded Symmetry of Information. Lecture Notes in Computer Science, 2004, , 463-475.	1.3	4
434	Computational Analogues of Entropy. Lecture Notes in Computer Science, 2003, , 200-215.	1.3	61

#	Article	IF	Citations
435	Underapproximation for Model-Checking Based on Random Cryptographic Constructions. , 2007, , 339-351.		1
436	Worst-Case to Average-Case Reductions Revisited. Lecture Notes in Computer Science, 2007, , 569-583.	1.3	10
437	Impossibility Results on Weakly Black-Box Hardness Amplification. Lecture Notes in Computer Science, 2007, , 400-411.	1.3	1
438	Cracks in the Defenses: Scouting Out Approaches on Circuit Lower Bounds. , 2008, , 3-10.		3
439	The Complexity of Local List Decoding. Lecture Notes in Computer Science, 2008, , 455-468.	1.3	13
440	Limitations of Hardness vs. Randomness under Uniform Reductions. Lecture Notes in Computer Science, 2008, , 469-482.	1.3	13
442	Random Low Degree Polynomials are Hard to Approximate. Lecture Notes in Computer Science, 2009, , 366-377.	1.3	2
443	Extractors Using Hardness Amplification. Lecture Notes in Computer Science, 2009, , 462-475.	1.3	4
445	On the Complexity of Non-adaptively Increasing the Stretch of Pseudorandom Generators. Lecture Notes in Computer Science, 2011, , 522-539.	1.3	4
447	Almost k-Wise Independent Sets Establish Hitting Sets for Width-3 1-Branching Programs. Lecture Notes in Computer Science, 2011, , 120-133.	1.3	5
448	Pseudo-random Graphs and Bit Probe Schemes with One-Sided Error. Lecture Notes in Computer Science, 2011, , 50-63.	1.3	3
449	Improving the Space-Bounded Version of Muchnikâ€™s Conditional Complexity Theorem via â€œNaiveâ€• Derandomization. Lecture Notes in Computer Science, 2011, , 64-76.	1.3	8
450	An Introduction to Randomness Extractors. Lecture Notes in Computer Science, 2011, , 21-41.	1.3	48
451	On the Optimal Compression of Sets in PSPACE. Lecture Notes in Computer Science, 2011, , 65-77.	1.3	3
452	Space-Bounded Kolmogorov Extractors. Lecture Notes in Computer Science, 2012, , 266-277.	1.3	3
453	On TC0 Lower Bounds for the Permanent. Lecture Notes in Computer Science, 2012, , 420-432.	1.3	1
454	Optimal Hitting Sets for Combinatorial Shapes. Lecture Notes in Computer Science, 2012, , 423-434.	1.3	1
455	A Survey of Data Structures in the Bitprobe Model. Lecture Notes in Computer Science, 2013, , 303-318.	1.3	15

#	Article	IF	Citations
456	Naturally Rehearsing Passwords. Lecture Notes in Computer Science, 2013, , 361-380.	1.3	14
457	Fine-Grained Cryptography. Lecture Notes in Computer Science, 2016, , 533-562.	1.3	15
461	Hardness Amplification for Errorless Heuristics. , 2007, , .		1
462	Almost-Everywhere Circuit Lower Bounds from Non-Trivial Derandomization. , 2020, , .		11
463	Guest Column. ACM SIGACT News, 2009, 40, 27-44.	0.1	7
464	Typically-correct derandomization. ACM SIGACT News, 2010, 41, 57-72.	0.1	5
465	XOR lemmas for resilient functions against polynomials. , 2020, , .		3
466	Strong average-case lower bounds from non-trivial derandomization. , 2020, , .		12
467	Sharp threshold results for computational complexity. , 2020, , .		12
468	Exponentially Faster Shortest Paths in the Congested Clique. , 2020, , .		3
469	Average-Case Complexity. Foundations and Trends in Theoretical Computer Science, 2006, 2, 1-106.	0.3	77
470	Pairwise Independence and Derandomization. Foundations and Trends in Theoretical Computer Science, 2005, 1, 237-301.	0.3	37
471	Arithmetic Circuits: A survey of recent results and open questions. Foundations and Trends in Theoretical Computer Science, 2009, 5, 207-388.	0.3	172
472	Pseudo-finite hard instances for a student-teacher game with a Nisan-Wigderson generator. Logical Methods in Computer Science, 2012, 8, .	0.4	27
473	Lower Bounds on van der Waerden Numbers: Randomized- and Deterministic-Constructive. Electronic Journal of Combinatorics, 2011, 18, .	0.4	2
474	Title is missing!. Theory of Computing, 2008, 4, 137-168.	0.5	55
475	Title is missing!. Theory of Computing, 2011, 7, 177-184.	0.5	9
476	Title is missing!. Theory of Computing, 2012, 8, 231-238.	0.5	5

#	Article	IF	Citations
477	Title is missing!. Theory of Computing, 2013, 9, 441-470.	0.5	1
478	Title is missing!. Theory of Computing, 2017, 13, 1-23.	0.5	3
479	Determinant versus permanent. , 2007, , 985-997.		7
487	Lower Bounds for Arithmetic Circuits via the Hankel Matrix. Computational Complexity, 2021, 30, 1.	0.3	0
488	The combinatorial game N ofil played on Steiner triple systems. Journal of Combinatorial Designs, 0, , .	0.6	0
489	Pseudorandomness. Lecture Notes in Computer Science, 2000, , 687-704.	1.3	1
490	On Distribution-Specific Learning with Membership Queries versus Pseudorandom Generation. Lecture Notes in Computer Science, 2000, , 336-347.	1.3	0
491	The First-Order Isomorphism Theorem. Lecture Notes in Computer Science, 2001, , 70-82.	1.3	6
492	Quantum Computation Relative to Oracles. , 2001, , 273-288.		0
493	Probabilistically Checkable Proofs the Easy Way. , 2002, , 337-351.		2
494	Nearly Bounded Error Probabilistic Sets. Lecture Notes in Computer Science, 2003, , 213-226.	1.3	0
495	On Proving Circuit Lower Bounds against the Polynomial-Time Hierarchy: Positive and Negative Results. Lecture Notes in Computer Science, 2003, , 202-211.	1.3	4
496	Random Access to Advice Strings and Collapsing Results. Lecture Notes in Computer Science, 2004, , 209-220.	1.3	0
497	Pseudorandomnessâ€"Part II. IAS/Park City Mathematics Series, 2004, , 287-314.	0.5	0
498	Arthur-Merlin Games and the Problem of Isomorphism Testing. Lecture Notes in Computer Science, 2005, , 495-506.	1.3	0
499	Computational Complexity Since 1980. Lecture Notes in Computer Science, 2005, , 19-47.	1.3	1
500	Reconstructive Dispersers and Hitting Set Generators. Lecture Notes in Computer Science, 2005, , 460-471.	1.3	3
501	Simple Extractors via Constructions of Cryptographic Pseudo-random Generators. Lecture Notes in Computer Science, 2005, , 115-127.	1.3	6

#	Article	IF	Citations
503	Non-black-box Techniques in Cryptography. Lecture Notes in Computer Science, 2006, , 1-1.	1.3	7
504	SIGACT news complexity theory column 53. ACM SIGACT News, 2006, 37, 47-55.	0.1	0
505	Lower Bounds for Swapping Arthur and Merlin. Lecture Notes in Computer Science, 2007, , 449-463.	1.3	4
507	Uniform Derandomization from Pathetic Lower Bounds. Lecture Notes in Computer Science, 2010, , 380-393.	1.3	2
508	On the Hardness against Constant-Depth Linear-Size Circuits. Lecture Notes in Computer Science, 2010, , 13-22.	1.3	1
509	The Complexity of Explicit Constructions. Lecture Notes in Computer Science, 2010, , 372-375.	1.3	0
510	Randomisation and Derandomisation in Descriptive Complexity Theory. Lecture Notes in Computer Science, 2010, , 275-289.	1.3	0
512	Correlation Bounds for Poly-size $mbox{m AC}^0$ Circuits with n 1â€‰â^’â€‰o(1) Symmetric Gates. Lecture Notes in Computer Science, 2011, , 640-651.	1.3	4
513	The Unified Theory of Pseudorandomness. , 2011, , .		4
514	When Formulas Freeze: Phase Transitions in Computation. , 2011, , 723-818.		0
515	The Grand Unified Theory of Computation. , 2011, , 223-299.		0
516	Interaction and Pseudorandomness. , 2011, , 506-562.		0
517	Memory, Paths, and Games. , 2011, , 300-350.		0
518	The Deep Question: P vs. NP. , 2011, , 173-222.		0
520	Needles in a Haystack: the Class NP. , 2011, , 94-126.		0
521	Counting, Sampling, and Statistical Physics. , 2011, , 651-722.		0
522	Insights and Algorithms. , 2011, , 41-93.		0
524	Optimization and Approximation. , 2011, , 351-449.		0

#	Article	IF	Citations
525	Quantum Computation. , 2011, , 819-910.		0
526	Randomized Algorithms. , 2011, , 450-505.		0
527	Who is the Hardest One of All? NP-Completeness. , 2011, , 127-172.		0
528	Randomisation and Derandomisation in Descriptive Complexity Theory. Logical Methods in Computer Science, 2011, 7, .	0.4	0
529	A Sufficient Condition for Sets Hitting the Class of Read-Once Branching Programs of Width 3. Lecture Notes in Computer Science, 2012, , 406-418.	1.3	1
530	Formalizing Randomized Matching Algorithms. Logical Methods in Computer Science, 2012, 8, .	0.4	3
532	Amortized Communication Complexity of an Equality Predicate. Lecture Notes in Computer Science, 2013, , 212-223.	1.3	1
533	On Efficient Constructions of Short Lists Containing Mostly Ramsey Graphs. Lecture Notes in Computer Science, 2013, , 205-211.	1.3	0
534	Learning Reductions to Sparse Sets. Lecture Notes in Computer Science, 2013, , 243-253.	1.3	1
535	On the Limits of Depth Reduction at Depth 3 Over Small Finite Fields. Lecture Notes in Computer Science, 2014, , 177-188.	1.3	0
536	Proving Circuit Lower Bounds in High Uniform Classes. Interdisciplinary Information Sciences, 2014, 20, 1-26.	0.4	0
537	A Selection of Lower Bounds for Arithmetic Circuits. , 2014, , 77-115.		3
538	Optimal bounds on the approximation of boolean functions with consequences on the concept of hardness. Lecture Notes in Computer Science, 1996, , 319-330.	1.3	0
539	Using hard problems to derandomize algorithms: An incomplete survey. Lecture Notes in Computer Science, 1997, , 165-173.	1.3	0
540	Injective Trapdoor Functions via Derandomization: How Strong is Rudichâ€™s Black-Box Barrier?. Lecture Notes in Computer Science, 2018, , 421-447.	1.3	2
541	Credimus. Studies in Economic Design, 2019, , 141-152.	0.0	0
542	Robust Distributed Pseudorandom Functions for mNP Access Structures. Lecture Notes in Computer Science, 2019, , 107-126.	1.3	0
543	Some Estimated Likelihoods for Computational Complexity. Lecture Notes in Computer Science, 2019, , 9-26.	1.3	3

#	Article	IF	Citations
544	CCA-Secure (Puncturable) KEMs from Encryption with Non-Negligible Decryption Errors. Lecture Notes in Computer Science, 2020, , 159-190.	1.3	6
546	On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions. Lecture Notes in Computer Science, 2020, , 41-86.	1.3	1
547	On Perfect Correctness in (Lockable) Obfuscation. Lecture Notes in Computer Science, 2020, , 229-259.	1.3	1
548	Characterizing Deterministic-Prover Zero Knowledge. Lecture Notes in Computer Science, 2020, , 535-566.	1.3	2
549	Separation Between Read-once Oblivious Algebraic Branching Programs (ROABPs) and Multilinear Depth-three Circuits. ACM Transactions on Computation Theory, 2020, 12, 1-27.	0.7	1
550	Simple and Efficient Batch Verification Techniques for Verifiable Delay Functions. Lecture Notes in Computer Science, 2021, , 382-414.	1.3	5
551	Re-pairing brackets. , 2020, , .		0
552	Circuit Lower Bounds for MCSP from Local Pseudorandom Generators. ACM Transactions on Computation Theory, 2020, 12, 1-27.	0.7	3
554	Symmetry of Information and Nonuniform Lower Bounds. Lecture Notes in Computer Science, 2007, , 315-327.	1.3	1
555	Arthur and Merlin as Oracles. Lecture Notes in Computer Science, 2008, , 229-240.	1.3	0
556	Compression of samplable sources. , 0, , .		2
557	Is it Easier to Prove Theorems that are Guaranteed to be True?. , 2020, , .		4
558	Nearly Optimal Pseudorandomness From Hardness. , 2020, , .		6
559	On Exponential-Time Hypotheses, Derandomization, and Circuit Lower Bounds: Extended Abstract. , 2020, , .		1
561	Fooling Polytopes. Journal of the ACM, 2022, 69, 1-37.	2.2	0
563	Quantum learning algorithms imply circuit lower bounds. , 2022, , .		2
564	Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits. , 2022, , .		4
565	Hardness vs Randomness, Revised: Uniform, Non-Black-Box, and Instance-Wise. , 2022, , .		3

#	Article	IF	Citations
566	Improved Extractors for Small-Space Sources. , 2022, , .		3
567	Demystifying the border of depth-3 algebraic circuits. , 2022, , .		1
568	Expander-Based Cryptography Meets Natural Proofs. Computational Complexity, 2022, 31, 1.	0.3	0
569	Efficient Construction of Rigid Matrices Using an NP Oracle. SIAM Journal on Computing, 0, , FOCS19-102-FOCS19-134.	1.0	0
570	Homodyne detection in quantum optics: deterministic extractors and quantum random number generators on â€˜vacuum fluctuationsâ€™. Laser Physics, 2022, 32, 055202.	1.2	0
571	Regarding Two Conjectures on Clique and Biclique Partitions. Electronic Journal of Combinatorics, 2021, 28, .	0.4	1
572	Guest Column. ACM SIGACT News, 2021, 52, 56-73.	0.1	0
573	SIGACT News Complexity Theory Column 112. ACM SIGACT News, 2022, 53, 58-58.	0.1	0
574	Derandomization from Algebraic Hardness. SIAM Journal on Computing, 2022, 51, 315-335.	1.0	3
579	Pseudorandomness and combinatorial constructions. , 2007, , 1111-1136.		2
581	Strong Average-Case Circuit Lower Bounds from Nontrivial Derandomization. SIAM Journal on Computing, 2022, 51, STOC20-115-STOC20-173.	1.0	3
582	A Note on Perfect Correctness by Derandomization. Journal of Cryptology, 2022, 35, .	2.8	0
584	Recent Advances in Randomness Extraction. Entropy, 2022, 24, 880.	2.2	0
585	Nearly Optimal Pseudorandomness from Hardness. Journal of the ACM, 2022, 69, 1-55.	2.2	1
586	On Secret Sharing, Randomness, andÂRandom-less Reductions forÂSecret Sharing. Lecture Notes in Computer Science, 2022, , 327-354.	1.3	0
592	NP-Hardness of Learning Programs and Partial MCSP. , 2022, , .		7
593	Unstructured Hardness to Average-Case Randomness. , 2022, , .		3
594	Hardness Self-Amplification from Feasible Hard-Core Sets. , 2022, , .		3

#	Article	IF	Citations
597	Black-Box Separations forÂNon-interactive Classical Commitments inÂaÂQuantum World. Lecture Notes in Computer Science, 2023, , 144-172.	1.3	0
598	On Exponential-time Hypotheses, Derandomization, and Circuit Lower Bounds. Journal of the ACM, 2023, 70, 1-62.	2.2	1
599	Toward Basing Cryptography on the Hardness of EXP. Communications of the ACM, 2023, 66, 91-99.	4.5	0
600	Optimal Explicit Small-Depth Formulas for the Coin Problem. , 2023, , .		0
601	Guest Column: New ways of studying the BPP = P conjecture. ACM SIGACT News, 2023, 54, 44-69.	0.1	0
602	Unprovability of Strong Complexity Lower Bounds in Bounded Arithmetic. , 2023, , .		0
603	When Arthur Has Neither Random Coins Nor Time to Spare: Superfast Derandomization of Proof Systems. , 2023, , .		1
604	Hard Languages in NP â̂© coNP and NIZK Proofs from Unstructured Hardness. , 2023, , .		0
605	The Power of Natural Properties as Oracles. Computational Complexity, 2023, 32, .	0.3	1
606	Extractors: Low Entropy Requirements Colliding withÂNon-malleability. Lecture Notes in Computer Science, 2023, , 580-610.	1.3	0
607	Non-Black-Box Worst-Case to Average-Case Reductions Within (mathsf{NP}). SIAM Journal on Computing, 2023, 52, FOCS18-349-FOCS18-382.	1.0	0
608	Derandomization vs Refutation: A Unified Framework for Characterizing Derandomization. , 2023, , .		0
609	Certified Hardness vs. Randomness for Log-Space. , 2023, , .		1
610	Polynomial-Time Pseudodeterministic Construction of Primes. , 2023, , .		0
611	Nondeterministic Quasi-Polynomial Time is Average-Case Hard for (extsf{ACC}) Circuits. SIAM Journal on Computing, 0, , FOCS19-332-FOCS19-397.	1.0	0