Oded Goldreich

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4468442/publications.pdf

Version: 2024-02-01

244 papers	21,161 citations	50566 48 h-index	20023 121 g-index
271 all docs	271 docs citations	271 times ranked	5294 citing authors

#	Article	IF	Citations
1	Improved bounds on the AN-complexity of $$O(1)$$-linear functions. Computational Complexity, 2022, 31, .	0.2	0
2	Universal locally verifiable codes and 3-round interactive proofs of proximity for CSP. Theoretical Computer Science, 2021, 878-879, 83-101.	0.5	2
3	Flexible Models for Testing Graph Properties. Lecture Notes in Computer Science, 2020, , 352-362.	1.0	1
4	Pseudo-mixing Time of Random Walks. Lecture Notes in Computer Science, 2020, , 363-373.	1.0	0
5	The Subgraph Testing Model. ACM Transactions on Computation Theory, 2020, 12, 1-32.	0.4	0
6	On the Size of Depth-Three Boolean Circuits for Computing Multilinear Functions. Lecture Notes in Computer Science, 2020, , 41-86.	1.0	1
7	Constant-Round Interactive Proof Systems for AC0[2] and NC1. Lecture Notes in Computer Science, 2020, , 326-351.	1.0	2
8	On the Effect of the Proximity Parameter on Property Testers. Lecture Notes in Computer Science, 2020, , 36-40.	1.0	0
9	On the Relation Between the Relative Earth Mover Distance and the Variation Distance (an Exposition). Lecture Notes in Computer Science, 2020, , 141-151.	1.0	0
10	On Constant-Depth Canonical Boolean Circuits for Computing Multilinear Functions. Lecture Notes in Computer Science, 2020, , 306-325.	1.0	0
11	Worst-Case to Average-Case Reductions for Subclasses of P. Lecture Notes in Computer Science, 2020, , 249-295.	1.0	4
12	Two Comments on Targeted Canonical Derandomizers. Lecture Notes in Computer Science, 2020, , 24-35.	1.0	1
13	On Emulating Interactive Proofs with Public Coins. Lecture Notes in Computer Science, 2020, , 178-198.	1.0	0
14	On the Communication Complexity Methodology for Proving Lower Bounds on the Query Complexity of Property Testing. Lecture Notes in Computer Science, 2020, , 87-118.	1.0	3
15	Bridging a Small Gap in the Gap Amplification of Assignment Testers. Lecture Notes in Computer Science, 2020, , 9-16.	1.0	0
16	Hierarchy Theorems for Testing Properties in Size-Oblivious Query Complexity. Computational Complexity, 2019, 28, 709-747.	0.2	2
17	On the foundations of cryptography. , 2019, , .		5
18	On the impact of cryptography on complexity theory. , 2019, , .		0

#	Article	IF	Citations
19	Testing graphs in vertex-distribution-free models. , 2019, , .		2
20	Strong Locally Testable Codes with Relaxed Local Decoders. ACM Transactions on Computation Theory, 2019, 11, 1-38.	0.4	3
21	On Doubly-Efficient Interactive Proof Systems. Foundations and Trends in Theoretical Computer Science, 2018, 13, 157-246.	2.0	4
22	Matrix rigidity of random Toeplitz matrices. Computational Complexity, 2018, 27, 305-350.	0.2	6
23	Counting t-Cliques: Worst-Case to Average-Case Reductions and Direct Interactive Proof Systems. , 2018, , .		13
24	Proofs of proximity for context-free languages and read-once branching programs. Information and Computation, 2018, 261, 175-201.	0.5	1
25	On Learning and Testing Dynamic Environments. Journal of the ACM, 2017, 64, 1-90.	1.8	14
26	On Sample-Based Testers. ACM Transactions on Computation Theory, 2016, 8, 1-54.	0.4	8
27	Estimating Simple Graph Parameters in Sublinear Time. , 2016, , 650-653.		0
28	Matrix rigidity of random toeplitz matrices. , 2016, , .		6
29	Special Issue on the 10th Theory of Cryptography Conference: Editorâ€™s Foreword. Computational Complexity, 2016, 25, 563-565.	0.2	0
30	Two-sided error proximity oblivious testing. Random Structures and Algorithms, 2016, 48, 341-383.	0.6	3
31	Testing Bipartiteness in the Dense-Graph Model. , 2016, , 2212-2216.		0
32	Testing Bipartiteness of Graphs in Sublinear Time. , 2016, , 2216-2219.		0
33	Input-Oblivious Proof Systems and a Uniform Complexity Perspective on P/poly. ACM Transactions on Computation Theory, 2015, 7, 1-13.	0.4	2
34	On Sample-Based Testers. , 2015, , .		8
35	Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs. Lecture Notes in Computer Science, 2015, , 666-677.	1.0	5
36	Estimating Simple Graph Parameters in Sublinear Time. , 2015, , 1-5.		0

#	Article	IF	Citations
37	Testing Bipartiteness of Graphs in Sublinear Time. , 2015, , 1-5.		0
38	On Learning and Testing Dynamic Environments. , 2014, , .		2
39	On derandomizing algorithms that err extremely rarely. , 2014, , .		13
40	Finding cycles and trees in sublinear time. Random Structures and Algorithms, 2014, 45, 139-184.	0.6	23
41	More Constructions of Lossy and Correlation-Secure Trapdoor Functions. Journal of Cryptology, 2013, 26, 39-74.	2.1	40
42	Enhancements of Trapdoor Permutations. Journal of Cryptology, 2013, 26, 484-512.	2.1	27
43	On the possibilities and limitations of pseudodeterministic algorithms. , 2013, , .		7
44	A theory of goal-oriented communication. Journal of the ACM, 2012, 59, 1-65.	1.8	30
45	On struggle and competition in scientic fields. ACM SIGACT News, 2012, 43, 43-60.	0.1	1
46	On the (im)possibility of obfuscating programs. Journal of the ACM, 2012, 59, 1-48.	1.8	334
47	Hierarchy Theorems for Property Testing. Computational Complexity, 2012, 21, 129-192.	0.2	9
48	Special issue from RANDOMâ€™09: Editorsâ€™ Foreword. Computational Complexity, 2012, 21, 1-1.	0.2	0
49	The tensor product of two good codes is not necessarily robustly testable. Information Processing Letters, 2012, 112, 351-355.	0.4	11
50	Two-Sided Error Proximity Oblivious Testing. Lecture Notes in Computer Science, 2012, , 565-578.	1.0	3
51	Title is missing!. Theory of Computing, 2012, 8, 231-238.	0.3	5
52	On Constructing 1-1 One-Way Functions. Lecture Notes in Computer Science, 2011, , 13-25.	1.0	9
53	Proving Computational Ability. Lecture Notes in Computer Science, 2011, , 6-12.	1.0	2
54	Algorithmic Aspects of Property Testing in the Dense Graphs Model. SIAM Journal on Computing, 2011, 40, 376-445.	0.8	13

#	Article	IF	Citations
55	On Proximity-Oblivious Testing. SIAM Journal on Computing, 2011, 40, 534-566.	0.8	33
56	A theory of goal-oriented communication. , 2011, , .		0
57	Finding the Shortest Move-Sequence in the Graph-Generalized 15-Puzzle Is NP-Hard. Lecture Notes in Computer Science, 2011, , 1-5.	1.0	18
58	Candidate One-Way Functions Based on Expander Graphs. Lecture Notes in Computer Science, 2011, , 76-87.	1.0	25
59	Using the FGLSS-Reduction to Prove Inapproximability Results for Minimum Vertex Cover in Hypergraphs. Lecture Notes in Computer Science, 2011, , 88-97.	1.0	3
60	On Probabilistic versus Deterministic Provers in the Definition of Proofs of Knowledge. Lecture Notes in Computer Science, 2011, , 114-123.	1.0	8
61	In a World of P=BPP. Lecture Notes in Computer Science, 2011, , 191-232.	1.0	12
62	Three XOR-Lemmas â€" An Exposition. Lecture Notes in Computer Science, 2011, , 248-272.	1.0	15
63	On Yaoâ€™s XOR-Lemma. Lecture Notes in Computer Science, 2011, , 273-301.	1.0	27
64	A Sample of Samplers: A Computational Perspective on Sampling. Lecture Notes in Computer Science, 2011, , 302-332.	1.0	21
65	Bravely, Moderately: A Common Theme in Four Recent Works. Lecture Notes in Computer Science, 2011, , 373-389.	1.0	3
66	Basing Non-Interactive Zero-Knowledge on (Enhanced) Trapdoor Permutations: The State of the Art. Lecture Notes in Computer Science, 2011, , 406-421.	1.0	20
67	Basic Facts about Expander Graphs. Lecture Notes in Computer Science, 2011, , 451-464.	1.0	4
68	Randomness and Computation. Lecture Notes in Computer Science, 2011, , 507-539.	1.0	10
69	On Security Preserving Reductions â€" Revised Terminology. Lecture Notes in Computer Science, 2011, , 540-546.	1.0	2
70	Collision-Free Hashing from Lattice Problems. Lecture Notes in Computer Science, 2011, , 30-39.	1.0	16
71	On Testing Expansion in Bounded-Degree Graphs. Lecture Notes in Computer Science, 2011, , 68-75.	1.0	33
72	Proximity Oblivious Testing and the Role of Invariances. Lecture Notes in Computer Science, 2011, , 579-592.	1.0	5

#	Article	IF	Citations
73	Contemplations on Testing Graph Properties. Lecture Notes in Computer Science, 2011, , 547-554.	1.0	1
74	Simplified Derandomization of BPP Using a Hitting Set Generator. Lecture Notes in Computer Science, 2011, , 59-67.	1.0	7
75	Average Case Complexity, Revisited. Lecture Notes in Computer Science, 2011, , 422-450.	1.0	1
76	Short Locally Testable Codes and Proofs. Lecture Notes in Computer Science, 2011, , 333-372.	1.0	4
77	On the Circuit Complexity of Perfect Hashing. Lecture Notes in Computer Science, 2011, , 26-29.	1.0	0
78	Another Motivation for Reducing the Randomness Complexity of Algorithms. Lecture Notes in Computer Science, 2011, , 555-560.	1.0	1
79	Another Proof That $mathcal{BPP}subseteq mathcal{PH}$ (and More). Lecture Notes in Computer Science, 2011, , 40-53.	1.0	5
80	From Logarithmic Advice to Single-Bit Advice. Lecture Notes in Computer Science, 2011, , 109-113.	1.0	2
81	The GGM Construction Does NOT Yield Correlation Intractable Function Ensembles. Lecture Notes in Computer Science, 2011, , 98-108.	1.0	0
82	Notes on Levinâ€™s Theory of Average-Case Complexity. Lecture Notes in Computer Science, 2011, , 233-247.	1.0	6
83	Complexity Theory. Oberwolfach Reports, 2010, 6, 2787-2850.	0.0	0
84	On The Randomness Complexity of Property Testing. Computational Complexity, 2010, 19, 99-133.	0.2	12
85	On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions andÂTheirÂBenefits. Journal of Cryptology, 2010, 23, 1-36.	2.1	7
86	Erratum for. , 2010, , .		4
87	On the Implementation of Huge Random Objects. SIAM Journal on Computing, 2010, 39, 2761-2822.	0.8	20
88	More Constructions of Lossy and Correlation-Secure Trapdoor Functions. Lecture Notes in Computer Science, 2010, , 279-295.	1.0	74
89	On Testing Computability by Small Width OBDDs. Lecture Notes in Computer Science, 2010, , 574-587.	1.0	17
90	Algorithmic Aspects of Property Testing in the Dense Graphs Model. Lecture Notes in Computer Science, 2010, , 295-305.	1.0	4

#	ARTICLE	IF	CITATIONS
91	Short Locally Testable Codes and Proofs: A Survey in Two Parts. Lecture Notes in Computer Science, 2010, , 65-104.	1.0	13
92	Introduction to Testing Graph Properties. Lecture Notes in Computer Science, 2010, , 105-141.	1.0	16
93	The Program of the Mini-Workshop. Lecture Notes in Computer Science, 2010, , 6-12.	1.0	0
94	Hierarchy Theorems for Property Testing. Lecture Notes in Computer Science, 2010, , 289-294.	1.0	1
95	A Brief Introduction to Property Testing. Lecture Notes in Computer Science, 2010, , 1-5.	1.0	4
96	On proximity oblivious testing. , 2009, , .		17
97	Universal Arguments and their Applications. SIAM Journal on Computing, 2009, 38, 1661-1694.	0.8	64
98	Hierarchy Theorems for Property Testing. Lecture Notes in Computer Science, 2009, , 504-519.	1.0	4
99	Algorithmic Aspects of Property Testing in the Dense Graphs Model. Lecture Notes in Computer Science, 2009, , 520-533.	1.0	1
100	On our duties as scientists. ACM SIGACT News, 2009, 40, 53-59.	0.1	0
101	Preface to the Special Issue from Randomâ€™06. Computational Complexity, 2008, 17, 1-2.	0.2	0
102	Approximating average parameters of graphs. Random Structures and Algorithms, 2008, 32, 473-493.	0.6	45
103	Probabilistic Proof Systems: A Primer. Foundations and Trends in Theoretical Computer Science, 2008, 3, 1-91.	2.0	2
104	Special Issue On Worst-case Versus Average-case Complexity Editorsâ€™ Foreword. Computational Complexity, 2007, 16, 325-330.	0.2	3
105	On Expected Probabilistic Polynomial-Time Adversaries: A Suggestion for Restricted Definitions and Their Benefits. , 2007, , 174-193.		8
106	On the Randomness Complexity of Property Testing. Lecture Notes in Computer Science, 2007, , 509-524.	1.0	4
107	Special Issue on Randomness and Complexity. SIAM Journal on Computing, 2006, 36, ix-xi.	0.8	0
108	Robust PCPs of Proximity, Shorter PCPs, and Applications to Coding. SIAM Journal on Computing, 2006, 36, 889-974.	0.8	144

#	Article	IF	Citations
109	Session-Key Generation Using Human Passwords Only. Journal of Cryptology, 2006, 19, 241-340.	2.1	40
110	Lower bounds for linear locally decodable codes and private information retrieval. Computational Complexity, 2006, 15, 263-296.	0.2	32
111	On basing one-way functions on NP-hardness. , 2006, , .		42
112	Locally testable codes and PCPs of almost-linear length. Journal of the ACM, 2006, 53, 558-655.	1.8	96
113	On Promise Problems: A Survey. Lecture Notes in Computer Science, 2006, , 254-290.	1.0	42
114	Concurrent Zero-Knowledge with Timing, Revisited. Lecture Notes in Computer Science, 2006, , 27-87.	1.0	2
115	Foundations of Cryptography â€“ A Primer. Foundations and Trends in Theoretical Computer Science, 2005, 1, 1-116.	2.0	39
116	The random oracle methodology, revisited. Journal of the ACM, 2004, 51, 557-594.	1.8	614
117	Robust pcps of proximity, shorter pcps and applications to coding. , 2004, , .		52
118	On the Random-Oracle Methodology as Applied to Length-Restricted Signature Schemes. Lecture Notes in Computer Science, 2004, , 40-57.	1.0	40
119	Cryptography and cryptographic protocols. Distributed Computing, 2003, 16, 177-199.	0.7	42
120	Almost k-wise independence versus k-wise independence. Information Processing Letters, 2003, 88, 107-110.	0.4	31
121	Three theorems regarding testing graph properties. Random Structures and Algorithms, 2003, 23, 23-57.	0.6	114
122	Bounds on 2-Query Codeword Testing. Lecture Notes in Computer Science, 2003, , 216-227.	1.0	15
123	On interactive proofs with a laconic prover. Computational Complexity, 2002, 11, 1-53.	0.2	63
124	Derandomization That Is Rarely Wrong from Short Advice That Is Typically Good. Lecture Notes in Computer Science, 2002, , 209-223.	1.0	22
125	Property Testing in Massive Graphs. Massive Computing, 2002, , 123-147.	0.4	8
126	On the (Im)possibility of Obfuscating Programs. Lecture Notes in Computer Science, 2001, , 1-18.	1.0	703

#	Article	IF	Citations
127	Session-Key Generation Using Human Passwords Only. Lecture Notes in Computer Science, 2001, , 408-432.	1.0	136
128	On Interactive Proofs with a Laconic Prover. Lecture Notes in Computer Science, 2001, , 334-345.	1.0	7
129	On the Limits of Nonapproximability of Lattice Problems. Journal of Computer and System Sciences, 2000, 60, 540-563.	0.9	112
130	Uniform Generation of NP-Witnesses Using an NP-Oracle. Information and Computation, 2000, 163, 510-526.	0.5	57
131	Testing Monotonicity. Combinatorica, 2000, 20, 301-337.	0.6	148
132	Resettable zero-knowledge (extended abstract). , 2000, , .		109
133	Learning Polynomials with Queries: The Highly Noisy Case. SIAM Journal on Discrete Mathematics, 2000, 13, 535-570.	0.4	82
134	A Combinatorial Consistency Lemma with Application to Proving the PCP Theorem. SIAM Journal on Computing, 2000, 29, 1132-1154.	0.8	24
135	Computational Sample Complexity. SIAM Journal on Computing, 2000, 29, 854-879.	0.8	15
136	Pseudorandomness. Lecture Notes in Computer Science, 2000, , 687-704.	1.0	1
137	The graph clustering problem has a perfect zero-knowledge interactive proof. Information Processing Letters, 1999, 69, 201-206.	0.4	7
138	A Sublinear Bipartiteness Tester for Bounded Degree Graphs. Combinatorica, 1999, 19, 335-373.	0.6	106
139	Computational Indistinguishability: A Sample Hierarchy. Journal of Computer and System Sciences, 1999, 59, 253-269.	0.9	2
140	Chinese remaindering with errors. , 1999, , .		53
141	Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, 1999, , .	0.6	130
142	Stateless Evaluation of Pseudorandom Functions: Security Beyond the Birthday Barrier. Lecture Notes in Computer Science, 1999, , 270-287.	1.0	28
143	Can Statistical Zero Knowledge Be Made Non-interactive? or On the Relationship of SZK and NISZK. Lecture Notes in Computer Science, 1999, , 467-484.	1.0	36
144	Improved Testing Algorithms for Monotonicity. Lecture Notes in Computer Science, 1999, , 97-108.	1.0	68

#	Article	IF	Citations
145	Improved Derandomization of BPP Using a Hitting Set Generator. Lecture Notes in Computer Science, 1999, , 131-137.	1.0	10
146	The Foundations of Modern Cryptography. Algorithms and Combinatorics, 1999, , 1-37.	0.6	6
147	On the complexity of interactive proofs with bounded communication. Information Processing Letters, 1998, 67, 205-214.	0.4	57
148	Efficient approximation of product distributions. Random Structures and Algorithms, 1998, 13, 1-16.	0.6	37
149	Computational indistinguishability: Algorithms vs. circuits. Theoretical Computer Science, 1998, 191, 215-218.	0.5	6
150	Fault-tolerant Computation in the Full Information Model. SIAM Journal on Computing, 1998, 27, 506-544.	0.8	32
151	Computational Complexity and Knowledge Complexity. SIAM Journal on Computing, 1998, 27, 1116-1141.	0.8	11
152	Free Bits, PCPs, and Nonapproximability---Towards Tight Results. SIAM Journal on Computing, 1998, 27, 804-915.	0.8	354
153	Private information retrieval. Journal of the ACM, 1998, 45, 965-981.	1.8	1,059
154	Property testing and its connection to learning and approximation. Journal of the ACM, 1998, 45, 653-750.	1.8	702
155	The random oracle methodology, revisited (preliminary version). , 1998, , .		393
156	A sublinear bipartiteness tester for bounded degree graphs. , 1998, , .		13
157	Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. , 1998, , .		64
158	Self-delegation with controlled propagation â€" or â€" What if you lose your laptop. Lecture Notes in Computer Science, 1998, , 153-168.	1.0	22
159	Efficient approximation of product distributions. , 1998, 13, 1.		5
160	Property testing in bounded degree graphs. , 1997, , .		76
161	On the foundations of modern cryptography. Lecture Notes in Computer Science, 1997, , 46-74.	1.0	28
162	Public-key cryptosystems from lattice reduction problems. Lecture Notes in Computer Science, 1997, , 112-131.	1.0	251

#	Article	IF	Citations
163	Probabilistic proof systems â€" A survey. Lecture Notes in Computer Science, 1997, , 595-611.	1.0	2
164	Tiny families of functions with random properties: A quality-size trade-off for hashing. Random Structures and Algorithms, 1997, 11, 315-343.	0.6	54
165	On universal learning algorithms. Information Processing Letters, 1997, 63, 131-136.	0.4	3
166	Tiny families of functions with random properties: A quality-size trade-off for hashing. , 1997, 11, 315.		12
167	A Taxonomy of Proof Systems. , 1997, , 109-134.		6
168	A combinatorial consistency lemma with application to proving the PCP theorem. Lecture Notes in Computer Science, 1997, , 67-84.	1.0	5
169	How to construct constant-round zero-knowledge proof systems for NP. Journal of Cryptology, 1996, 9, 167-189.	2.1	135
170	On-line/off-line digital signatures. Journal of Cryptology, 1996, 9, 35-67.	2.1	245
171	Software protection and simulation on oblivious RAMs. Journal of the ACM, 1996, 43, 431-473.	1.8	1,109
172	On the Composition of Zero-Knowledge Proof Systems. SIAM Journal on Computing, 1996, 25, 169-192.	0.8	280
173	The future of computational complexity theory: part I. ACM SIGACT News, 1996, 27, 6-12.	0.1	1
174	Adaptively secure multi-party computation. , 1996, , .		334
175	On-line/off-line digital signatures. , 1996, 9, 35.		11
176	How To Construct Constant-Round Zero-Knowledge Proof Systems for NP. Journal of Cryptology, 1996, 9, 167.	2.1	187
177	Theory of computing. ACM Computing Surveys, 1996, 28, 218.	16.1	54
178	Lower bounds for sampling algorithms for estimating the average. Information Processing Letters, 1995, 53, 17-25.	0.4	60
179	Incremental cryptography and application to virus protection. , 1995, , .		92
180	Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs. Lecture Notes in Computer Science, 1995, , 325-338.	1.0	22

#	Article	IF	Citations
181	Probabilistic Proof Systems. , 1995, , 1395-1406.		5
182	Tiny families of functions with random properties (preliminary version). , 1994, , .		8
183	Computational complexity and knowledge complexity (extended abstract). , 1994, , .		6
184	Definitions and properties of zero-knowledge proof systems. Journal of Cryptology, 1994, 7, 1-32.	2.1	414
185	The random oracle hypothesis is false. Journal of Computer and System Sciences, 1994, 49, 24-39.	0.9	55
186	Hashing Functions can Simplify Zero-Knowledge Protocol Design (too). BRICS Report Series, 1994, 1, .	0.2	13
187	A taxonomy of proof systems (part 2). ACM SIGACT News, 1994, 25, 22-30.	0.1	0
188	Addendum to â€œsimple constructions of almost k-wise independent random variablesâ€• Random Structures and Algorithms, 1993, 4, 119-120.	0.6	13
189	Bounds on tradeoffs between randomness and communication complexity. Computational Complexity, 1993, 3, 141-167.	0.2	18
190	Randomness in interactive proofs. Computational Complexity, 1993, 3, 319-354.	0.2	38
191	A perfect zero-knowledge proof system for a problem equivalent to the discrete logarithm. Journal of Cryptology, 1993, 6, 97-116.	2.1	26
192	A uniform-complexity treatment of encryption and zero-knowledge. Journal of Cryptology, 1993, 6, 21-53.	2.1	84
193	Asynchronous secure computation. , 1993, , .		121
194	On the Existence of Pseudorandom Generators. SIAM Journal on Computing, 1993, 22, 1163-1175.	0.8	88
195	A taxonomy of proof systems (part 1). ACM SIGACT News, 1993, 24, 2-13.	0.1	2
196	Critique of some trends in the TCS community in light of two controversies. ACM SIGACT News, 1992, 23, 44-46.	0.1	0
197	Sparse pseudorandom distributions. Random Structures and Algorithms, 1992, 3, 163-174.	0.6	13
198	Simple Constructions of Almost k-wise Independent Random Variables. Random Structures and Algorithms, 1992, 3, 289-304.	0.6	382

#	Article	IF	Citations
199	On the theory of average case complexity. Journal of Computer and System Sciences, 1992, 44, 193-219.	0.9	117
200	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.	0.9	353
201	On Defining Proofs of Knowledge. , 1992, , 390-420.		285
202	On the complexity of computation in the presence of link failures: the case of a ring. Distributed Computing, 1991, 5, 121-131.	0.7	14
203	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.	0.7	81
204	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.	1.8	802
205	A fair protocol for signing contracts. IEEE Transactions on Information Theory, 1990, 36, 40-46.	1.5	235
206	A note on computational indistinguishability. Information Processing Letters, 1990, 34, 277-281.	0.4	46
207	An improved parallel algorithm for integer GCD. Algorithmica, 1990, 5, 1-10.	1.0	31
208	On the number of monochromatic close pairs of beads in a rosary. Discrete Mathematics, 1990, 80, 59-68.	0.4	0
209	The best of both worlds: guaranteeing termination in fast randomized byzantine agreement protocols. Information Processing Letters, 1990, 36, 45-49.	0.4	26
210	Everything Provable is Provable in Zero-Knowledge. Lecture Notes in Computer Science, 1990, , 37-56.	1.0	103
211	On the composition of zero-knowledge proof systems. , 1990, , 268-282.		54
212	A trade-off between information and communication in broadcast protocols. Journal of the ACM, 1990, 37, 238-256.	1.8	86
213	On the Existence of Pseudorandom Generators. Lecture Notes in Computer Science, 1990, , 146-162.	1.0	2
214	On the power of two-point based sampling. Journal of Complexity, 1989, 5, 96-106.	0.7	146
215	On-Line/Off-Line Digital Signatures. , 1989, , 263-275.		144
216	Sparse Pseudorandom Distributions. , 1989, , 113-127.		6

#	Article	IF	Citations
217	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.	1.0	3
218	RSA and Rabin Functions: Certain Parts are as Hard as the Whole. SIAM Journal on Computing, 1988, 17, 194-209.	0.8	275
219	Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. SIAM Journal on Computing, 1988, 17, 230-261.	0.8	418
220	A tradeoff between information and communication in broadcast protocols. , 1988, , 369-379.		7
221	Interactive proof systems: Provers that never fail and random selection. , 1987, , .		30
222	Electing a leader in a ring with link failures. Acta Informatica, 1987, 24, 79-91.	0.5	18
223	On the time-complexity of broadcast in radio networks: an exponential gap between determinism randomization. , 1987, , .		69
224	Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. , 1986, , .		342
225	Proofs that Release Minimum Knowledge. , 1986, , 639-650.		1
226	How to construct random functions. Journal of the ACM, 1986, 33, 792-807.	1.8	1,417
227	Towards a Theory of Software Protection (Extended Abstract). , 1986, , 426-439.		5
228	How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design (Extended Abstract). , 1986, , 171-185.		56
229	Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme. , 1986, , 104-110.		52
230	A fair protocol for signing contracts. Lecture Notes in Computer Science, 1985, , 43-52.	1.0	17
231	A randomized protocol for signing contracts. Communications of the ACM, 1985, 28, 637-647.	3.3	948
232	The bit extraction problem or t-resilient functions. , 1985, , .		241
233	Unbiased bits from sources of weak randomness and probabilistic communication complexity. , 1985, , .		52
234	On the Security of Ping-Pong Protocols when Implemented using the RSA (Extended Abstract). , 1985, , 58-72.		8

#	Article	IF	Citations
235	The Bit Security of Modular Squaring given Partial Factorization of the Modulos. , 1985, , 448-457.		7
236	On the np-completeness of certain network testing problems. Networks, 1984, 14, 1-24.	1.6	87
237	On the Cryptographic Applications of Random Functions (Extended Abstract). , 1984, , 276-288.		57
238	RSA/Rabin least significant bits are $$ frac{1} {2} + frac{1} {{poly left({log N} ight)}} $$ secure (Extended Abstract). , 1984, , 303-313.		6
239	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 /O		2
240	A Simple Protocol for Signing Contracts. , 1984, , 133-136.		40
241	Electronic Wallet. , 1984, , 383-386.		25
242	On Concurrent Identification Protocols (Extended Abstract). , 1984, , 387-396.		0
243	DES-like functions can generate the alternating group. IEEE Transactions on Information Theory, 1983, 29, 863-865.	1.5	29
244	The minimum-length generator sequence problem is NP-hard. Journal of Algorithms, 1981, 2, 311-313.	0.9	67