Eyal Kushilevitz

List of Publications by Year in descending order

78 papers	4,284 citations	172386 29 h-index	118793 62 g-index
78 all docs	78 docs citations	78 times ranked	1456 citing authors

#	Article	IF	Citations
1	Private information retrieval. Journal of the ACM, 1998, 45, 965-981.	1.8	1,059
2	Learning Decision Trees Using the Fourier Spectrum. SIAM Journal on Computing, 1993, 22, 1331-1348.	0.8	232
3	Communication Complexity. Advances in Computers, 1997, , 331-360.	1.2	230
4	An $Omega(Dlog (N/D))$ Lower Bound for Broadcast in Radio Networks. SIAM Journal on Computing, 1998, 27, 702-712.	0.8	229
5	Protecting Data Privacy in Private Information Retrieval Schemes. Journal of Computer and System Sciences, 2000, 60, 592-629.	0.9	188
6	Cryptography in NC^0. SIAM Journal on Computing, 2006, 36, 845-888.	0.8	135
7	A Zero-One Law for Boolean Privacy. SIAM Journal on Discrete Mathematics, 1991, 4, 36-47.	0.4	117
8	Perfect Constant-Round Secure Computation via Perfect Randomizing Polynomials. Lecture Notes in Computer Science, 2002, , 244-256.	1.0	108
9	Cryptography with constant computational overhead. , 2008, , .		100
10	From Secrecy to Soundness: Efficient Verification via Secure Computation. Lecture Notes in Computer Science, 2010, , 152-163.	1.0	99
11	Amortized Communication Complexity. SIAM Journal on Computing, 1995, 24, 736-750.	0.8	90
12	COMPUTATIONALLY PRIVATE RANDOMIZING POLYNOMIALS AND THEIR APPLICATIONS. Computational Complexity, 2006, 15, 115-162.	0.2	83
13	General constructions for information-theoretic private information retrieval. Journal of Computer and System Sciences, 2005, 71, 213-247.	0.9	80
14	Zero-Knowledge Proofs from Secure Multiparty Computation. SIAM Journal on Computing, 2009, 39, 1121-1152.	0.8	80
15	Learning functions represented as multiplicity automata. Journal of the ACM, 2000, 47, 506-530.	1.8	77
16	Cryptography from Anonymity. , 2006, , .		77
17	On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions. Lecture Notes in Computer Science, 2003, , 68-86.	1.0	74
18	On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. Journal of Cryptology, 2006, 19, 135-167.	2.1	63

#	Article	IF	Citations
19	Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning. Proceedings on Privacy Enhancing Technologies, 2021, 2021, 188-208.	2.3	63
20	A communication-privacy tradeoff for modular addition. Information Processing Letters, 1993, 45, 205-210.	0.4	49
21	How to Garble Arithmetic Circuits. , 2011, , .		46
22	Information-Theoretically Secure Protocols and Security under Composition. SIAM Journal on Computing, 2010, 39, 2090-2112.	0.8	45
23	On the Cryptographic Complexity of the Worst Functions. Lecture Notes in Computer Science, 2014, , 317-342.	1.0	43
24	Fractional Covers and Communication Complexity. SIAM Journal on Discrete Mathematics, 1995, 8, 76-92.	0.4	42
25	Reducibility and Completeness in Private Computations. SIAM Journal on Computing, 2000, 29, 1189-1208.	0.8	41
26	Extracting Correlations. , 2009, , .		39
27	On Pseudorandom Generators with Linear Stretch in NC0. Computational Complexity, 2008, 17, 38-69.	0.2	38
28	Share Conversion and Private Information Retrieval. , 2012, , .		38
29	Secure Multiparty Computation with Minimal Interaction. Lecture Notes in Computer Science, 2010, , 577-594.	1.0	38
30	Online Learning versus Offline Learning. Machine Learning, 1997, 29, 45-63.	3.4	36
31	Cryptography with Constant Input Locality. Journal of Cryptology, 2009, 22, 429-469.	2.1	35
32	Encoding Functions with Constant Online Rate or How to Compress Garbled Circuits Keys. Lecture Notes in Computer Science, 2013, , 166-184.	1.0	35
33	Private computation using a PEZ dispenser. Theoretical Computer Science, 2003, 306, 69-84.	0.5	33
34	Secret sharing over infinite domains. Journal of Cryptology, 1993, 6, 87-95.	2.1	32
35	On the Hardness of Information-Theoretic Multiparty Computation. Lecture Notes in Computer Science, 2004, , 439-455.	1.0	29
36	Computation in Noisy Radio Networks. SIAM Journal on Discrete Mathematics, 2005, 19, 96-108.	0.4	26

#	Article	IF	Citations
37	On the structure of the privacy hierarchy. Journal of Cryptology, 1994, 7, 53-60.	2.1	24
38	Private Computations over the Integers. SIAM Journal on Computing, 1995, 24, 376-386.	0.8	23
39	A Randomness-Rounds Tradeoff in Private Computation. SIAM Journal on Discrete Mathematics, 1998, 11, 61-80.	0.4	23
40	On Achieving the â€œBest of Both Worldsâ€•in Secure Multiparty Computation. SIAM Journal on Computing, 2011, 40, 122-141.	0.8	23
41	How to Garble Arithmetic Circuits. SIAM Journal on Computing, 2014, 43, 905-929.	0.8	23
42	Randomness in Private Computations. SIAM Journal on Discrete Mathematics, 1997, 10, 647-661.	0.4	22
43	Cryptography with Constant Input Locality. Lecture Notes in Computer Science, 2007, , 92-110.	1.0	22
44	A simple algorithm for learning O(log n)-term DNF. Information Processing Letters, 1997, 61, 289-292.	0.4	20
45	Characterizing Linear Size Circuits in Terms of Privacy. Journal of Computer and System Sciences, 1999, 58, 129-136.	0.9	19
46	Robust Pseudorandom Generators. Lecture Notes in Computer Science, 2013, , 576-588.	1.0	19
47	Distribution-Free Property Testing. Lecture Notes in Computer Science, 2003, , 302-317.	1.0	18
48	Testing monotonicity over graph products. Random Structures and Algorithms, 2008, 33, 44-67.	0.6	16
49	On Pseudorandom Generators with Linear Stretch in NC0Â. Lecture Notes in Computer Science, 2006, , 260-271.	1.0	15
50	On learning Read-k-Satisfy-j DNF. , 1994, , .		14
51	Randomness versus Fault-Tolerance. Journal of Cryptology, 2000, 13, 107-142.	2.1	13
52	The Linear-Array Conjecture in Communication Complexity Is False. Combinatorica, 1999, 19, 241-254.	0.6	12
53	On Learning Read-k-Satisfy-j DNF. SIAM Journal on Computing, 1998, 27, 1515-1530.	0.8	11
54	Computing Functions of a Shared Secret. SIAM Journal on Discrete Mathematics, 2000, 13, 324-345.	0.4	11

#	Article	IF	Citations
55	Testing Monotonicity over Graph Products. Lecture Notes in Computer Science, 2004, , 721-732.	1.0	11
56	A Randomness-Rounds Tradeoff in Private Computation. , 1994, , 397-410.		10
57	Randomness vs. fault-tolerance. , 1997, , .		9
58	On the complexity of communication complexity. , 2009, , .		9
59	Encoding Functions with Constant Online Rate, or How to Compress Garbled Circuit Keys. SIAM Journal on Computing, 2015, 44, 433-466.	0.8	9
60	Distribution-Free Connectivity Testing. Lecture Notes in Computer Science, 2004, , 393-404.	1.0	9
61	Amortizing randomness in private multiparty computations. , 1998, , .		8
62	A Lower Bound for Distribution-Free Monotonicity Testing. Lecture Notes in Computer Science, 2005, , 330-341.	1.0	8
63	On Fully Secure MPC with Solitary Output. Lecture Notes in Computer Science, 2019, , 312-340.	1.0	8
64	Randomness in private computations. , 1996, , .		6
65	Distribution-Free Connectivity Testing for Sparse Graphs. Algorithmica, 2008, 51, 24-48.	1.0	6
66	On learning visual concepts and DNF formulae. Machine Learning, 1996, 24, 65-85.	3.4	5
67	Amortizing Randomness in Private Multiparty Computations. SIAM Journal on Discrete Mathematics, 2003, 16, 533-544.	0.4	5
68	The Communication Complexity of Set-Disjointness with Small Sets and 0-1 Intersection. , 2009, , .		4
69	Partition arguments in multiparty communication complexity. Theoretical Computer Science, 2011, 412, 2611-2622.	0.5	4
70	Choosing, Agreeing, and Eliminating in Communication Complexity. Computational Complexity, 2014, 23, 1-42.	0.2	3
71	Minimizing Locality of One-Way Functions via Semi-private Randomized Encodings. Journal of Cryptology, 2018, 31, 1-22.	2.1	3
72	Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. SIAM Journal on Discrete Mathematics, 2021, 35, 465-484.	0.4	3

#	Article	IF	Citations
73	Partition Arguments in Multiparty Communication Complexity. Lecture Notes in Computer Science, 2009, , 390-402.	1.0	2
74	The Query Complexity of Finding Local Minima in the Lattice. Information and Computation, 2001, 171, 69-83.	0.5	1
75	From randomizing polynomials to parallel algorithms. , 2012, , .		1
76	Choosing, Agreeing, and Eliminating in Communication Complexity. Lecture Notes in Computer Science, 2010, , 451-462.	1.0	1
77	Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. Lecture Notes in Computer Science, 2019, , 386-406.	1.0	1
78	CNF-FSS andÂlts Applications. Lecture Notes in Computer Science, 2022, , 283-314.	1.0	1