

Eyal Kushilevitz

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/10739973/publications.pdf>

Version: 2024-02-01

78
papers

4,284
citations

172207

29
h-index

118652

62
g-index

78
all docs

78
docs citations

78
times ranked

1456
citing authors

#	ARTICLE	IF	CITATIONS
1	CNF-FSS and Its Applications. Lecture Notes in Computer Science, 2022, , 283-314.	1.0	1
2	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
3	Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning. Proceedings on Privacy Enhancing Technologies, 2021, 2021, 188-208.	2.3	63
4	Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. Lecture Notes in Computer Science, 2019, , 386-406.	1.0	1
5	On Fully Secure MPC with Solitary Output. Lecture Notes in Computer Science, 2019, , 312-340.	1.0	8
6	Minimizing Locality of One-Way Functions via Semi-private Randomized Encodings. Journal of Cryptology, 2018, 31, 1-22.	2.1	3
7	Encoding Functions with Constant Online Rate, or How to Compress Garbled Circuit Keys. SIAM Journal on Computing, 2015, 44, 433-466.	0.8	9
8	How to Garble Arithmetic Circuits. SIAM Journal on Computing, 2014, 43, 905-929.	0.8	23
9	Choosing, Agreeing, and Eliminating in Communication Complexity. Computational Complexity, 2014, 23, 1-42.	0.2	3
10	On the Cryptographic Complexity of the Worst Functions. Lecture Notes in Computer Science, 2014, , 317-342.	1.0	43
11	Robust Pseudorandom Generators. Lecture Notes in Computer Science, 2013, , 576-588.	1.0	19
12	Encoding Functions with Constant Online Rate or How to Compress Garbled Circuits Keys. Lecture Notes in Computer Science, 2013, , 166-184.	1.0	35
13	From randomizing polynomials to parallel algorithms. , 2012, , .		1
14	Share Conversion and Private Information Retrieval. , 2012, , .		38
15	How to Garble Arithmetic Circuits. , 2011, , .		46
16	On Achieving the "Best of Both Worlds" in Secure Multiparty Computation. SIAM Journal on Computing, 2011, 40, 122-141.	0.8	23
17	Partition arguments in multiparty communication complexity. Theoretical Computer Science, 2011, 412, 2611-2622.	0.5	4
18	Information-Theoretically Secure Protocols and Security under Composition. SIAM Journal on Computing, 2010, 39, 2090-2112.	0.8	45

#	ARTICLE	IF	CITATIONS
19	From Secrecy to Soundness: Efficient Verification via Secure Computation. Lecture Notes in Computer Science, 2010, , 152-163.	1.0	99
20	Secure Multiparty Computation with Minimal Interaction. Lecture Notes in Computer Science, 2010, , 577-594.	1.0	38
21	Choosing, Agreeing, and Eliminating in Communication Complexity. Lecture Notes in Computer Science, 2010, , 451-462.	1.0	1
22	On the complexity of communication complexity. , 2009, , .		9
23	Cryptography with Constant Input Locality. Journal of Cryptology, 2009, 22, 429-469.	2.1	35
24	Zero-Knowledge Proofs from Secure Multiparty Computation. SIAM Journal on Computing, 2009, 39, 1121-1152.	0.8	80
25	Extracting Correlations. , 2009, , .		39
26	The Communication Complexity of Set-Disjointness with Small Sets and 0-1 Intersection. , 2009, , .		4
27	Partition Arguments in Multiparty Communication Complexity. Lecture Notes in Computer Science, 2009, , 390-402.	1.0	2
28	On Pseudorandom Generators with Linear Stretch in NC0. Computational Complexity, 2008, 17, 38-69.	0.2	38
29	Distribution-Free Connectivity Testing for Sparse Graphs. Algorithmica, 2008, 51, 24-48.	1.0	6
30	Testing monotonicity over graph products. Random Structures and Algorithms, 2008, 33, 44-67.	0.6	16
31	Cryptography with constant computational overhead. , 2008, , .		100
32	Cryptography with Constant Input Locality. Lecture Notes in Computer Science, 2007, , 92-110.	1.0	22
33	Cryptography from Anonymity. , 2006, , .		77
34	Cryptography in NC^0 . SIAM Journal on Computing, 2006, 36, 845-888.	0.8	135
35	On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. Journal of Cryptology, 2006, 19, 135-167.	2.1	63
36	COMPUTATIONALLY PRIVATE RANDOMIZING POLYNOMIALS AND THEIR APPLICATIONS. Computational Complexity, 2006, 15, 115-162.	0.2	83

#	ARTICLE	IF	CITATIONS
37	On Pseudorandom Generators with Linear Stretch in NC. Lecture Notes in Computer Science, 2006, , 260-271.	1.0	15
38	General constructions for information-theoretic private information retrieval. Journal of Computer and System Sciences, 2005, 71, 213-247.	0.9	80
39	Computation in Noisy Radio Networks. SIAM Journal on Discrete Mathematics, 2005, 19, 96-108.	0.4	26
40	A Lower Bound for Distribution-Free Monotonicity Testing. Lecture Notes in Computer Science, 2005, , 330-341.	1.0	8
41	On the Hardness of Information-Theoretic Multiparty Computation. Lecture Notes in Computer Science, 2004, , 439-455.	1.0	29
42	Distribution-Free Connectivity Testing. Lecture Notes in Computer Science, 2004, , 393-404.	1.0	9
43	Testing Monotonicity over Graph Products. Lecture Notes in Computer Science, 2004, , 721-732.	1.0	11
44	Private computation using a PEZ dispenser. Theoretical Computer Science, 2003, 306, 69-84.	0.5	33
45	Amortizing Randomness in Private Multiparty Computations. SIAM Journal on Discrete Mathematics, 2003, 16, 533-544.	0.4	5
46	On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions. Lecture Notes in Computer Science, 2003, , 68-86.	1.0	74
47	Distribution-Free Property Testing. Lecture Notes in Computer Science, 2003, , 302-317.	1.0	18
48	Perfect Constant-Round Secure Computation via Perfect Randomizing Polynomials. Lecture Notes in Computer Science, 2002, , 244-256.	1.0	108
49	The Query Complexity of Finding Local Minima in the Lattice. Information and Computation, 2001, 171, 69-83.	0.5	1
50	Protecting Data Privacy in Private Information Retrieval Schemes. Journal of Computer and System Sciences, 2000, 60, 592-629.	0.9	188
51	Randomness versus Fault-Tolerance. Journal of Cryptology, 2000, 13, 107-142.	2.1	13
52	Learning functions represented as multiplicity automata. Journal of the ACM, 2000, 47, 506-530.	1.8	77
53	Computing Functions of a Shared Secret. SIAM Journal on Discrete Mathematics, 2000, 13, 324-345.	0.4	11
54	Reducibility and Completeness in Private Computations. SIAM Journal on Computing, 2000, 29, 1189-1208.	0.8	41

#	ARTICLE	IF	CITATIONS
55	The Linear-Array Conjecture in Communication Complexity Is False. <i>Combinatorica</i> , 1999, 19, 241-254.	0.6	12
56	Characterizing Linear Size Circuits in Terms of Privacy. <i>Journal of Computer and System Sciences</i> , 1999, 58, 129-136.	0.9	19
57	A Randomness-Rounds Tradeoff in Private Computation. <i>SIAM Journal on Discrete Mathematics</i> , 1998, 11, 61-80.	0.4	23
58	An $\Omega(D \log(N/D))$ Lower Bound for Broadcast in Radio Networks. <i>SIAM Journal on Computing</i> , 1998, 27, 702-712.	0.8	229
59	On Learning Read- k -Satisfy- j DNF. <i>SIAM Journal on Computing</i> , 1998, 27, 1515-1530.	0.8	11
60	Private information retrieval. <i>Journal of the ACM</i> , 1998, 45, 965-981.	1.8	1,059
61	Amortizing randomness in private multiparty computations. , 1998, , .		8
62	Randomness vs. fault-tolerance. , 1997, , .		9
63	Randomness in Private Computations. <i>SIAM Journal on Discrete Mathematics</i> , 1997, 10, 647-661.	0.4	22
64	Communication Complexity. <i>Advances in Computers</i> , 1997, , 331-360.	1.2	230
65	Online Learning versus Offline Learning. <i>Machine Learning</i> , 1997, 29, 45-63.	3.4	36
66	A simple algorithm for learning $O(\log n)$ -term DNF. <i>Information Processing Letters</i> , 1997, 61, 289-292.	0.4	20
67	On learning visual concepts and DNF formulae. <i>Machine Learning</i> , 1996, 24, 65-85.	3.4	5
68	Randomness in private computations. , 1996, , .		6
69	Private Computations over the Integers. <i>SIAM Journal on Computing</i> , 1995, 24, 376-386.	0.8	23
70	Amortized Communication Complexity. <i>SIAM Journal on Computing</i> , 1995, 24, 736-750.	0.8	90
71	Fractional Covers and Communication Complexity. <i>SIAM Journal on Discrete Mathematics</i> , 1995, 8, 76-92.	0.4	42
72	On learning Read- k -Satisfy- j DNF. , 1994, , .		14

#	ARTICLE	IF	CITATIONS
73	On the structure of the privacy hierarchy. <i>Journal of Cryptology</i> , 1994, 7, 53-60.	2.1	24
74	A Randomness-Rounds Tradeoff in Private Computation. , 1994, , 397-410.		10
75	Secret sharing over infinite domains. <i>Journal of Cryptology</i> , 1993, 6, 87-95.	2.1	32
76	A communication-privacy tradeoff for modular addition. <i>Information Processing Letters</i> , 1993, 45, 205-210.	0.4	49
77	Learning Decision Trees Using the Fourier Spectrum. <i>SIAM Journal on Computing</i> , 1993, 22, 1331-1348.	0.8	232
78	A Zero-One Law for Boolean Privacy. <i>SIAM Journal on Discrete Mathematics</i> , 1991, 4, 36-47.	0.4	117