

Kai-Min Chung

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4002837/publications.pdf>

Version: 2024-02-01

52
papers

966
citations

516215

16
h-index

500791

28
g-index

53
all docs

53
docs citations

53
times ranked

492
citing authors

#	ARTICLE	IF	CITATIONS
1	Radius Margin Bounds for Support Vector Machines with the RBF Kernel. <i>Neural Computation</i> , 2003, 15, 2643-2681.	1.3	182
2	On Extractability Obfuscation. <i>Lecture Notes in Computer Science</i> , 2014, , 52-73.	1.0	111
3	An Optimal Algorithm for the Maximum-Density Segment Problem. <i>SIAM Journal on Computing</i> , 2005, 34, 373-387.	0.8	42
4	Large-Scale Secure Computation: Multi-party Computation for (Parallel) RAM Programs. <i>Lecture Notes in Computer Science</i> , 2015, , 742-762.	1.0	42
5	Oblivious Parallel RAM and Applications. <i>Lecture Notes in Computer Science</i> , 2016, , 175-204.	1.0	40
6	Decomposition Methods for Linear Support Vector Machines. <i>Neural Computation</i> , 2004, 16, 1689-1704.	1.3	36
7	Statistically-secure ORAM with $\text{poly}(\log^2 n)$ Overhead. <i>Lecture Notes in Computer Science</i> , 2014, , 62-81.	1.0	32
8	Distributed algorithms for the Lovász local lemma and graph coloring. <i>Distributed Computing</i> , 2017, 30, 261-280.	0.7	30
9	S-T Connectivity on Digraphs with a Known Stationary Distribution. <i>Computational Complexity, IEEE Annual Conference on</i> , 2007, , .	0.0	25
10	Cryptography for Parallel RAM from Indistinguishability Obfuscation. , 2016, , .		24
11	Constant-Round Concurrent Zero-Knowledge from Indistinguishability Obfuscation. <i>Lecture Notes in Computer Science</i> , 2015, , 287-307.	1.0	24
12	Delegating RAM Computations with Adaptive Soundness and Privacy. <i>Lecture Notes in Computer Science</i> , 2016, , 3-30.	1.0	24
13	Constant-Round Concurrent Zero Knowledge from P-Certificates. , 2013, , .		23
14	On the Complexity of Sorting in Magnetic Bubble Memory Systems. <i>IEEE Transactions on Computers</i> , 1980, C-29, 553-563.	2.4	21
15	Parallel Repetition Theorems for Interactive Arguments. <i>Lecture Notes in Computer Science</i> , 2010, , 19-36.	1.0	19
16	4-Round Resettable-Sound Zero Knowledge. <i>Lecture Notes in Computer Science</i> , 2014, , 192-216.	1.0	19
17	Tight Quantum Time-Space Tradeoffs for Function Inversion. , 2020, , .		17
18	Knowledge-Preserving Interactive Coding. , 2013, , .		16

#	ARTICLE	IF	CITATIONS
19	Distributed algorithms for the Lovász local lemma and graph coloring. , 2014, , .		16
20	On the Impossibility of Cryptography with Tamperable Randomness. Lecture Notes in Computer Science, 2014, , 462-479.	1.0	16
21	From Weak to Strong Zero-Knowledge and Applications. Lecture Notes in Computer Science, 2015, , 66-92.	1.0	16
22	On the Lattice Smoothing Parameter Problem. , 2013, , .		14
23	Simultaneous Resettability from One-Way Functions. , 2013, , .		14
24	On the Complexity of Permuting Records in Magnetic Bubble Memory Systems. IBM Journal of Research and Development, 1980, 24, 75-84.	3.2	13
25	On the Depth of Oblivious Parallel RAM. Lecture Notes in Computer Science, 2017, , 567-597.	1.0	12
26	Non-Black-Box Simulation from One-Way Functions and Applications to Resettable Security. SIAM Journal on Computing, 2016, 45, 415-458.	0.8	11
27	On the need for large Quantum depth. , 2020, , .		11
28	On Quantum Advantage in Information Theoretic Single-Server PIR. Lecture Notes in Computer Science, 2019, , 219-246.	1.0	10
29	A generalization of Ramsey theory for graphs. Discrete Mathematics, 1978, 21, 117-127.	0.4	9
30	S-T connectivity on digraphs with a known stationary distribution. ACM Transactions on Algorithms, 2011, 7, 1-21.	0.9	8
31	Non-black-box simulation from one-way functions and applications to resettable security. , 2013, , .		8
32	Game-Theoretic Fairness Meets Multi-party Protocols: The Case of Leader Election. Lecture Notes in Computer Science, 2021, , 3-32.	1.0	8
33	Game Theoretic Notions of Fairness in Multi-party Coin Toss. Lecture Notes in Computer Science, 2018, , 563-596.	1.0	8
34	Quantum encryption and generalized Shannon impossibility. Designs, Codes, and Cryptography, 2019, 87, 1961-1972.	1.0	7
35	Efficient Secure Two-Party Exponentiation. Lecture Notes in Computer Science, 2011, , 17-32.	1.0	7
36	A new permutation algorithm for bubble memories. Information Processing Letters, 1980, 10, 226-230.	0.4	6

#	ARTICLE	IF	CITATIONS
37	Narrowband active noise control using adaptive delay filter. IEEE Signal Processing Letters, 1998, 5, 309-311.	2.1	5
38	Decomposition methods for linear support vector machines. , 0, , .		5
39	On the Impossibility of Cryptography with Tamperable Randomness. Algorithmica, 2017, 79, 1052-1101.	1.0	5
40	Cryptography with Disposable Backdoors. Cryptography, 2019, 3, 22.	1.4	5
41	On the Complexity of Simulating Auxiliary Input. Lecture Notes in Computer Science, 2018, , 371-390.	1.0	5
42	The Randomness Complexity of Parallel Repetition. , 2011, , .		3
43	On the Concurrent Composition of Quantum Zero-Knowledge. Lecture Notes in Computer Science, 2021, , 346-374.	1.0	3
44	The Knowledge Tightness of Parallel Zero-Knowledge. Lecture Notes in Computer Science, 2012, , 512-529.	1.0	2
45	A Quantum-Proof Non-malleable Extractor. Lecture Notes in Computer Science, 2019, , 442-469.	1.0	2
46	Adaptively Secure Garbling Schemes for Parallel Computations. Lecture Notes in Computer Science, 2019, , 285-310.	1.0	2
47	Constant-Round Blind Classical Verification of Quantum Sampling. Lecture Notes in Computer Science, 2022, , 707-736.	1.0	2
48	Minimum number of steps for permutation in a bubble memory. Information Processing Letters, 1980, 11, 81-83.	0.4	1
49	Radius margin bounds for support vector machines with the RBF kernel. , 0, , .		1
50	Guest column. ACM SIGACT News, 2013, 44, 50-69.	0.1	1
51	On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Round. , 2022, , .		1
52	Interactive Leakage Chain Rule for Quantum Min-entropy. , 2019, , .		0