# Kai-Min Chung

## List of Publications by Year
in descending order

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

Version: 2024-02-01

|  |  | 516215 | 500791 |
|---|---|---|---|
| 52<br>papers | 966<br>citations | 16<br>h-index | 28<br>g-index |
| 53<br>all docs | 53<br>docs citations | 53<br>times ranked | 492<br>citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Round. , 2022, , . |  | 1 |
| 2 | Constant-Round Blind Classical Verification ofÂQuantum Sampling. Lecture Notes in Computer Science, 2022, , 707-736. | 1.0 | 2 |
| 3 | Game-Theoretic Fairness Meets Multi-party Protocols: The Case ofÂLeader Election. Lecture Notes in Computer Science, 2021, , 3-32. | 1.0 | 8 |
| 4 | On the Concurrent Composition of Quantum Zero-Knowledge. Lecture Notes in Computer Science, 2021, , 346-374. | 1.0 | 3 |
| 5 | Tight Quantum Time-Space Tradeoffs for Function Inversion. , 2020, , . |  | 17 |
| 6 | On the need for large Quantum depth. , 2020, , . |  | 11 |
| 7 | Cryptography with Disposable Backdoors. Cryptography, 2019, 3, 22. | 1.4 | 5 |
| 8 | On Quantum Advantage in Information Theoretic Single-Server PIR. Lecture Notes in Computer Science, 2019, , 219-246. | 1.0 | 10 |
| 9 | Interactive Leakage Chain Rule for Quantum Min-entropy. , 2019, , . |  | 0 |
| 10 | Quantum encryption and generalized Shannon impossibility. Designs, Codes, and Cryptography, 2019, 87, 1961-1972. | 1.0 | 7 |
| 11 | A Quantum-Proof Non-malleable Extractor. Lecture Notes in Computer Science, 2019, , 442-469. | 1.0 | 2 |
| 12 | Adaptively Secure Garbling Schemes for Parallel Computations. Lecture Notes in Computer Science, 2019, , 285-310. | 1.0 | 2 |
| 13 | Game Theoretic Notions of Fairness in Multi-party Coin Toss. Lecture Notes in Computer Science, 2018, , 563-596. | 1.0 | 8 |
| 14 | On the Complexity of Simulating Auxiliary Input. Lecture Notes in Computer Science, 2018, , 371-390. | 1.0 | 5 |
| 15 | On the Impossibility of Cryptography with Tamperable Randomness. Algorithmica, 2017, 79, 1052-1101. | 1.0 | 5 |
| 16 | On the Depth of Oblivious Parallel RAM. Lecture Notes in Computer Science, 2017, , 567-597. | 1.0 | 12 |
| 17 | Distributed algorithms for the LovÃ¡sz local lemma and graph coloring. Distributed Computing, 2017, 30, 261-280. | 0.7 | 30 |
| 18 | Non-Black-Box Simulation from One-Way Functions and Applications to Resettable Security. SIAM Journal on Computing, 2016, 45, 415-458. | 0.8 | 11 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Cryptography for Parallel RAM from Indistinguishability Obfuscation. , 2016, , . | | 24 |
| 20 | Oblivious Parallel RAM and Applications. Lecture Notes in Computer Science, 2016, , 175-204. | 1.0 | 40 |
| 21 | Delegating RAM Computations with Adaptive Soundness and Privacy. Lecture Notes in Computer Science, 2016, , 3-30. | 1.0 | 24 |
| 22 | From Weak to Strong Zero-Knowledge and Applications. Lecture Notes in Computer Science, 2015, , 66-92. | 1.0 | 16 |
| 23 | Constant-Round Concurrent Zero-Knowledge from Indistinguishability Obfuscation. Lecture Notes in Computer Science, 2015, , 287-307. | 1.0 | 24 |
| 24 | Large-Scale Secure Computation: Multi-party Computation for (Parallel) RAM Programs. Lecture Notes in Computer Science, 2015, , 742-762. | 1.0 | 42 |
| 25 | Distributed algorithms for the LovÃ¡sz local lemma and graph coloring. , 2014, , . | | 16 |
| 26 | Statistically-secure ORAM with $ilde{O}(log^2 n)$ Overhead. Lecture Notes in Computer Science, 2014, , 62-81. | 1.0 | 32 |
| 27 | On Extractability Obfuscation. Lecture Notes in Computer Science, 2014, , 52-73. | 1.0 | 111 |
| 28 | 4-Round Resettably-Sound Zero Knowledge. Lecture Notes in Computer Science, 2014, , 192-216. | 1.0 | 19 |
| 29 | On the Impossibility of Cryptography with Tamperable Randomness. Lecture Notes in Computer Science, 2014, , 462-479. | 1.0 | 16 |
| 30 | On the Lattice Smoothing Parameter Problem. , 2013, , . | | 14 |
| 31 | Knowledge-Preserving Interactive Coding. , 2013, , . | | 16 |
| 32 | Simultaneous Resettability from One-Way Functions. , 2013, , . | | 14 |
| 33 | Constant-Round Concurrent Zero Knowledge from P-Certificates. , 2013, , . | | 23 |
| 34 | Non-black-box simulation from one-way functions and applications to resettable security. , 2013, , . | | 8 |
| 35 | Guest column. ACM SIGACT News, 2013, 44, 50-69. | 0.1 | 1 |
| 36 | The Knowledge Tightness of Parallel Zero-Knowledge. Lecture Notes in Computer Science, 2012, , 512-529. | 1.0 | 2 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | The Randomness Complexity of Parallel Repetition. , 2011, , . | | 3 |
| 38 | S-T connectivity on digraphs with a known stationary distribution. ACM Transactions on Algorithms, 2011, 7, 1-21. | 0.9 | 8 |
| 39 | Efficient Secure Two-Party Exponentiation. Lecture Notes in Computer Science, 2011, , 17-32. | 1.0 | 7 |
| 40 | Parallel Repetition Theorems for Interactive Arguments. Lecture Notes in Computer Science, 2010, , 19-36. | 1.0 | 19 |
| 41 | S-T Connectivity on Digraphs with a Known Stationary Distribution. Computational Complexity, IEEE Annual Conference on, 2007, , . | 0.0 | 25 |
| 42 | An Optimal Algorithm for the Maximum-Density Segment Problem. SIAM Journal on Computing, 2005, 34, 373-387. | 0.8 | 42 |
| 43 | Decomposition Methods for Linear Support Vector Machines. Neural Computation, 2004, 16, 1689-1704. | 1.3 | 36 |
| 44 | Radius Margin Bounds for Support Vector Machines with the RBF Kernel. Neural Computation, 2003, 15, 2643-2681. | 1.3 | 182 |
| 45 | Narrowband active noise control using adaptive delay filter. IEEE Signal Processing Letters, 1998, 5, 309-311. | 2.1 | 5 |
| 46 | Minimum number of steps for permutation in a bubble memory. Information Processing Letters, 1980, 11, 81-83. | 0.4 | 1 |
| 47 | A new permutation algorithm for bubble memories. Information Processing Letters, 1980, 10, 226-230. | 0.4 | 6 |
| 48 | On the Complexity of Sorting in Magnetic Bubble Memory Systems. IEEE Transactions on Computers, 1980, C-29, 553-563. | 2.4 | 21 |
| 49 | On the Complexity of Permuting Records in Magnetic Bubble Memory Systems. IBM Journal of Research and Development, 1980, 24, 75-84. | 3.2 | 13 |
| 50 | A generalization of Ramsey theory for graphs. Discrete Mathematics, 1978, 21, 117-127. | 0.4 | 9 |
| 51 | Radius margin bounds for support vector machines with the RBF kernel. , 0, , . | | 1 |
| 52 | Decomposition methods for linear support vector machines. , 0, , . | | 5 |