Rafail Ostrovsky

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11290980/publications.pdf

Version: 2024-02-01

82 papers	5,917 citations	218381 26 h-index	123241 61 g-index
83 all docs	83 docs citations	83 times ranked	2829 citing authors

#	Article	IF	Citations
1	Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 2008, 38, 97-139.	0.8	1,172
2	Software protection and simulation on oblivious RAMs. Journal of the ACM, 1996, 43, 431-473.	1.8	1,109
3	Searchable symmetric encryption: Improved definitions and efficient constructions. Journal of Computer Security, 2011, 19, 895-934.	0.5	621
4	Perfect Non-interactive Zero Knowledge for NP. Lecture Notes in Computer Science, 2006, , 339-358.	1.0	236
5	Zero-knowledge from secure multiparty computation. , 2007, , .		232
6	Sequential Aggregate Signatures and Multisignatures Without Random Oracles. Lecture Notes in Computer Science, 2006, , 465-485.	1.0	228
7	Efficient Search for Approximate Nearest Neighbor in High Dimensional Spaces. SIAM Journal on Computing, 2000, 30, 457-474.	0.8	194
8	The Effectiveness of Lloyd-Type Methods for the k-Means Problem. , 2006, , .		125
9	New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM, 2012, 59, 1-35.	1.8	125
10	Perfect Zero-Knowledge Arguments for NP Using Any One-Way Permutation. Journal of Cryptology, 1998, 11, 87-108.	2.1	113
11	Round-Optimal Secure Two-Party Computation. Lecture Notes in Computer Science, 2004, , 335-354.	1.0	108
12	The effectiveness of lloyd-type methods for the k-means problem. Journal of the ACM, 2012, 59, 1-22.	1.8	84
13	Efficient Non-interactive Secure Computation. Lecture Notes in Computer Science, 2011, , 406-425.	1.0	83
14	Zero-Knowledge Proofs from Secure Multiparty Computation. SIAM Journal on Computing, 2009, 39, 1121-1152.	0.8	80
15	Efficient Arguments without Short PCPs. Computational Complexity, IEEE Annual Conference on, 2007, , .	0.0	79
16	Cryptography from Anonymity. , 2006, , .		77
17	Efficient and Non-interactive Non-malleable Commitment. Lecture Notes in Computer Science, 2001, , 40-59.	1.0	76
18	Private Searching on Streaming Data. Journal of Cryptology, 2007, 20, 397-430.	2.1	67

#	Article	IF	Citations
19	Constructing Non-malleable Commitments: A Black-Box Approach. , 2012, , .		58
20	Low distortion embeddings for edit distance. Journal of the ACM, 2007, 54, 23.	1.8	54
21	Round Efficiency of Multi-party Computation with a Dishonest Majority. Lecture Notes in Computer Science, 2003, , 578-595.	1.0	51
22	Fast Verification of Any Remote Procedure Call: Short Witness-Indistinguishable One-Round Proofs for NP. Lecture Notes in Computer Science, 2000, , 463-474.	1.0	48
23	Cryptography in the Multi-string Model. , 2007, , 323-341.		45
24	Reducibility and Completeness in Private Computations. SIAM Journal on Computing, 2000, 29, 1189-1208.	0.8	41
25	Polynomial-time approximation schemes for geometric min-sum median clustering. Journal of the ACM, 2002, 49, 139-156.	1.8	39
26	Extracting Correlations. , 2009, , .		39
27	Optimal Coding for Streaming Authentication and Interactive Communication. IEEE Transactions on Information Theory, 2015, 61, 133-145.	1.5	37
28	Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions. Lecture Notes in Computer Science, 2013, , 702-718.	1.0	37
29	Unconditionally-Secure Robust Secret Sharing with Compact Shares. Lecture Notes in Computer Science, 2012, , 195-208.	1.0	35
30	Adaptive Packet Routing for Bursty Adversarial Traffic. Journal of Computer and System Sciences, 2000, 60, 482-509.	0.9	34
31	Zero-one frequency laws. , 2010, , .		34
32	Identifying genetic relatives without compromising privacy. Genome Research, 2014, 24, 664-672.	2.4	30
33	Almost-Everywhere Secure Computation. , 2008, , 307-323.		30
34	Coding for Interactive Communication Correcting Insertions and Deletions. IEEE Transactions on Information Theory, 2017, 63, 6256-6270.	1.5	28
35	Identifying Cheaters without an Honest Majority. Lecture Notes in Computer Science, 2012, , 21-38.	1.0	27
36	Sequential Aggregate Signatures, Multisignatures, and Verifiably Encrypted Signatures Without Random Oracles. Journal of Cryptology, 2013, 26, 340-373.	2.1	26

#	Article	IF	Citations
37	Reusable Non-Interactive Secure Computation. Lecture Notes in Computer Science, 2019, , 462-488.	1.0	26
38	On Complete Primitives for Fairness. Lecture Notes in Computer Science, 2010, , 91-108.	1.0	23
39	Round Complexity of Authenticated Broadcast with a Dishonest Majority. , 2007, , .		22
40	Smooth Histograms for Sliding Windows. , 2007, , .		21
41	Privacy amplification with asymptotically optimal entropy loss. , 2010, , .		21
42	Effective Computations on Sliding Windows. SIAM Journal on Computing, 2010, 39, 2113-2131.	0.8	20
43	Characterizing Linear Size Circuits in Terms of Privacy. Journal of Computer and System Sciences, 1999, 58, 129-136.	0.9	19
44	Minimal Complete Primitives for Secure Multi-Party Computation. Journal of Cryptology, 2005, 18, 37-61.	2.1	19
45	Robust Pseudorandom Generators. Lecture Notes in Computer Science, 2013, , 576-588.	1.0	19
46	Stability Preserving Transformations: Packet Routing Networks with Edge Capacities and Speeds. Journal of Interconnection Networks, 2004, 05, 1-12.	0.6	18
47	Delayed-Input Non-Malleable Zero Knowledge and Multi-Party Coin Tossing in Four Rounds. Lecture Notes in Computer Science, 2017, , 711-742.	1.0	17
48	Visual cryptography on graphs. Journal of Combinatorial Optimization, 2011, 21, 47-66.	0.8	16
49	Minimal Complete Primitives for Secure Multi-party Computation. Lecture Notes in Computer Science, 2001, , 80-100.	1.0	14
50	Randomness versus Fault-Tolerance. Journal of Cryptology, 2000, 13, 107-142.	2.1	13
51	Cryptography in the Multi-string Model. Journal of Cryptology, 2014, 27, 506-543.	2.1	12
52	Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs. Lecture Notes in Computer Science, 2017, , 382-411.	1.0	12
53	Randomness vs. fault-tolerance. , 1997, , .		9
54	Measuring independence of datasets. , 2010, , .		9

#	Article	IF	Citations
55	Secure Message Transmission with Small Public Discussion. Lecture Notes in Computer Science, 2010, , 177-196.	1.0	9
56	On Succinct Arguments and Witness Encryption from Groups. Lecture Notes in Computer Science, 2020, , 776-806.	1.0	8
57	Log-Space Polynomial End-to-End Communication. SIAM Journal on Computing, 1998, 27, 1531-1549.	0.8	7
58	Subquadratic Approximation Algorithms for Clustering Problems in High Dimensional Spaces. Machine Learning, 2004, 56, 153-167.	3.4	6
59	Authenticated Adversarial Routing. Lecture Notes in Computer Science, 2009, , 163-182.	1.0	6
60	Secure Message Transmission by Public Discussion: A Brief Survey. Lecture Notes in Computer Science, 2011, , 126-141.	1.0	6
61	Succinct Non-Interactive Arguments via Linear Interactive Proofs. Journal of Cryptology, 2022, 35, 1.	2.1	6
62	Amortizing Randomness in Private Multiparty Computations. SIAM Journal on Discrete Mathematics, 2003, 16, 533-544.	0.4	5
63	Almost-Everywhere Secure Computation with Edge Corruptions. Journal of Cryptology, 2015, 28, 745-768.	2.1	5
64	Unconditionally Secure Computation with Reduced Interaction. Lecture Notes in Computer Science, 2016, , 420-447.	1.0	5
65	Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions. , 2007, , 444-459.		5
66	Asynchronous Throughput-Optimal Routing in Malicious Networks. Lecture Notes in Computer Science, 2010, , 236-248.	1.0	4
67	Smooth Histograms for Sliding Windows. , 2007, , .		4
68	A refined approximation for Euclidean k-means. Information Processing Letters, 2022, 176, 106251.	0.4	4
69	Privacy amplification with asymptotically optimal entropy loss. Journal of the ACM, 2014, 61, 1-28.	1.8	3
70	Efficient robust secret sharing from expander graphs. Cryptography and Communications, 2018, 10, 79-99.	0.9	3
71	DURASIFT. , 2019, , .		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	Round Complexity of Authenticated Broadcast with a Dishonest Majority. , 2007, , .		3
74	An architecture for a resilient cloud computing infrastructure. , 2013, , .		2
75	Secure Message Transmission With Small Public Discussion. IEEE Transactions on Information Theory, 2014, 60, 2373-2390.	1.5	2
76	Deterministic and Energy-Optimal Wireless Synchronization. ACM Transactions on Sensor Networks, 2014, 11, 1-25.	2.3	2
77	On the Black-box Use of Somewhat Homomorphic Encryption in NonInteractive Two-Party Protocols. SIAM Journal on Discrete Mathematics, 2016, 30, 266-295.	0.4	2
78	Oblivious Sampling with Applications to Two-Party k-Means Clustering. Journal of Cryptology, 2020, 33, 1362-1403.	2.1	1
79	Lower and Upper Bounds on the Randomness Complexity of Private Computations of AND. Lecture Notes in Computer Science, 2019, , 386-406.	1.0	1
80	Authenticated Adversarial Routing. Journal of Cryptology, 2014, 27, 636-771.	2.1	0
81	Efficient Error-Correcting Codes for Sliding Windows. SIAM Journal on Discrete Mathematics, 2020, 34, 904-937.	0.4	0
82	Secure End-to-End Communication with Optimal Throughput and Resilience against Malicious Adversary. Lecture Notes in Computer Science, 2013, , 403-417.	1.0	0