Gilles Brassard

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11111107/publications.pdf

Version: 2024-02-01

73 papers	24,593 citations	159585 30 h-index	144013 57 g-index
79 all docs	79 docs citations	79 times ranked	7899 citing authors

#	Article	IF	Citations
1	Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 1993, 70, 1895-1899.	7.8	10,750
2	Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Physical Review Letters, 1996, 76, 722-725.	7.8	2,318
3	Quantum cryptography without Bellâ€™s theorem. Physical Review Letters, 1992, 68, 557-559.	7.8	1,871
4	Experimental quantum cryptography. Journal of Cryptology, 1992, 5, 3-28.	2.8	1,507
5	Limitations on Practical Quantum Cryptography. Physical Review Letters, 2000, 85, 1330-1333.	7.8	1,016
6	Strengths and Weaknesses of Quantum Computing. SIAM Journal on Computing, 1997, 26, 1510-1523.	1.0	906
7	Privacy Amplification by Public Discussion. SIAM Journal on Computing, 1988, 17, 210-229.	1.0	694
8	Minimum disclosure proofs of knowledge. Journal of Computer and System Sciences, 1988, 37, 156-189.	1.2	657
9	Tight Bounds on Quantum Searching. Fortschritte Der Physik, 1998, 46, 493-505.	4.4	642
10	Secret-Key Reconciliation by Public Discussion. , 1993, , 410-423.		421
11	Quantum Cryptography. Scientific American, 1992, 267, 50-57.	1.0	289
12	Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial. Physical Review Letters, 2006, 96, 250401.	7.8	275
13	Experimental Quantum Cryptography. Lecture Notes in Computer Science, 1991, , 253-265.	1.3	241
14	Cost of Exactly Simulating Quantum Entanglement with Classical Communication. Physical Review Letters, 1999, 83, 1874-1877.	7.8	236
15	Quantum speed-up for unsupervised learning. Machine Learning, 2013, 90, 261-287.	5.4	140
16	Teleportation as a quantum computation. Physica D: Nonlinear Phenomena, 1998, 120, 43-47.	2.8	129
17	Quantum Pseudo-Telepathy. Foundations of Physics, 2005, 35, 1877-1907.	1.3	113
18	Practical Quantum Oblivious Transfer. , 1991, , 351-366.		103

#	Article	IF	Citations
19	Quantum Communication Complexity. Foundations of Physics, 2003, 33, 1593-1616.	1.3	90
20	Alambic: a privacy-preserving recommender system for electronic commerce. International Journal of Information Security, 2008, 7, 307-334.	3.4	89
21	Quantum computing without entanglement. Theoretical Computer Science, 2004, 320, 15-33.	0.9	84
22	Secure implementation of identification systems. Journal of Cryptology, 1991, 4, 175-183.	2.8	80
23	Quantum cryptanalysis of hash and claw-free functions. ACM SIGACT News, 1997, 28, 14-19.	0.1	69
24	An Update on Quantum Cryptography. , 1984, , 475-480.		63
25	Oracle Quantum Computing. Journal of Modern Optics, 1994, 41, 2521-2535.	1.3	60
26	Quantum clustering algorithms. , 2007, , .		55
27	Is information the key?. Nature Physics, 2005, 1, 2-4.	16.7	52
28	25 years of quantum cryptography. ACM SIGACT News, 1996, 27, 13-24.	0.1	48
29	Quantum Bit Commitment and Coin Tossing Protocols. , 1990, , 49-61.		45
30	On Computationally Secure Authentication Tags Requiring Short Secret Shared Keys. , 1983, , 79-86.		45
31	Constant-round perfect zero-knowledge computationally convincing protocols. Theoretical Computer Science, 1991, 84, 23-52.	0.9	42
32	Oblivious Transfers and Privacy Amplification. Journal of Cryptology, 2003, 16, 219-237.	2.8	36
33	Multiuser quantum key distribution using wavelength division multiplexing. , 2003, , .		35
34	Experimental loss-tolerant quantum coin flipping. Nature Communications, 2011, 2, 561.	12.8	32
35	Quantum public key distribution reinvented. ACM SIGACT News, 1987, 18, 51-53.	0.1	29
36	Entanglement cost of nonlocal measurements. Physical Review A, 2009, 80, .	2.5	27

#	Article	IF	Citations
37	Reduction of Quantum Entropy by Reversible Extraction of Classical Information. Journal of Modern Optics, 1994, 41, 2307-2314.	1.3	25
38	Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds. Lecture Notes in Computer Science, 1989, , 123-136.	1.3	23
39	Anonymous Quantum Communication. , 2007, , 460-473.		23
40	One-Way Group Actions. , 1990, , 94-107.		21
41	Merkle Puzzles in a Quantum World. Lecture Notes in Computer Science, 2011, , 391-410.	1.3	18
42	Oblivious Transfers and Privacy Amplification. Lecture Notes in Computer Science, 1997, , 334-347.	1.3	18
43	Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. Natural Computing, 2014, 13, 453-458.	3.0	17
44	Multi-party Pseudo-Telepathy. Lecture Notes in Computer Science, 2003, , 1-11.	1.3	16
45	Quantum Merkle Puzzles. , 2008, , .		13
46	Everything in NP can be argued in perfect zero-knowledge in a bounded number of rounds. , 1989, , 192-195.		13
47	A quantum jump in computer science. Lecture Notes in Computer Science, 1995, , 1-14.	1.3	12
48	Subquadratic zero-knowledge. Journal of the ACM, 1995, 42, 1169-1193.	2.2	11
49	Security Aspects of Practical Quantum Cryptography. Lecture Notes in Computer Science, 2000, , 289-299.	1.3	11
50	CLARISSE: A Machine Learning Tool to Initialize Student Models. Lecture Notes in Computer Science, 2002, , 718-728.	1.3	11
51	Sorting out zero-knowledge. , 1989, , 181-191.		10
52	Computationally convincing proofs of knowledge. , 1991, , 251-262.		7
53	Tight Bounds on Quantum Searching. , 2004, , 187-199.		7
54	New trends in quantum computing. Lecture Notes in Computer Science, 1996, , 1-10.	1.3	7

#	Article	IF	Citations
55	How convincing is your protocol?. ACM SIGACT News, 1991, 22, 5-12.	0.1	6
56	The conundrum of secure positioning. Nature, 2011, 479, 307-308.	27.8	5
57	Quantum information processing: The good, the bad and the ugly. Lecture Notes in Computer Science, 1997, , 337-341.	1.3	4
58	Exact Classical Simulation of the Quantum-Mechanical GHZ Distribution. IEEE Transactions on Information Theory, 2016, 62, 876-890.	2.4	4
59	Remote Sampling with Applications to General Entanglement Simulation. Entropy, 2019, 21, 92.	2.2	4
60	Classical, quantum and nonsignalling resources in bipartite games. Theoretical Computer Science, 2013, 486, 61-72.	0.9	3
61	Multi-particle entanglement via two-party entanglement. Journal of Physics A, 2001, 34, 6807-6814.	1.6	2
62	Quantum Cryptography Via Parametric Downconversion. , 2002, , 381-386.		2
63	Blind Electronic Commerce. Journal of Computer Security, 2006, 14, 535-559.	0.8	2
64	Noisy Interactive Quantum Communication. SIAM Journal on Computing, 2019, 48, 1147-1195.	1.0	2
65	Strict Hierarchy of Bell Theorems. , 2008, , .		1
66	Oblivious Transfer à la Merkle. , 2009, , .		1
67	Strict hierarchy among Bell Theorems. Theoretical Computer Science, 2013, 486, 4-10.	0.9	1
68	Cryptography in a Quantum World. Lecture Notes in Computer Science, 2016, , 3-16.	1.3	1
69	Simulating Equatorial Measurements on GHZ States with Finite Expected Communication Cost. Lecture Notes in Computer Science, 2013, , 65-73.	1.3	1
70	Classical, Quantum and Non-signalling Resources in Bipartite Games. , 2008, , .		0
71	Key Establishment Ã la Merkle in a Quantum World. Journal of Cryptology, 2019, 32, 601-634.	2.8	0
72	Quantum Cryptography. , 2011, , 1005-1010.		0

#	Article	IF	Citations
73	â€œPractical IPâ€•âŠ† MA. Lecture Notes in Computer Science, 1990, , 580-582.	1.3	0