

Daniele Micciancio

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/8771866/publications.pdf>

Version: 2024-02-01

82
papers

5,293
citations

186209

28
h-index

182361

51
g-index

86
all docs

86
docs citations

86
times ranked

1497
citing authors

#	ARTICLE	IF	CITATIONS
1	On the Security of Homomorphic Encryption on Approximate Numbers. Lecture Notes in Computer Science, 2021, , 648-677.	1.0	47
2	Homomorphic Encryption Standard. , 2021, , 31-62.		29
3	Semi-Parallel logistic regression for GWAS on encrypted data. BMC Medical Genomics, 2020, 13, 99.	0.7	16
4	Improved Discrete Gaussian and Subgaussian Analysis for Lattice Cryptography. Lecture Notes in Computer Science, 2020, , 623-651.	1.0	15
5	Interactive proofs for lattice problems. , 2019, , .		0
6	Homomorphic Encryption for Finite Automata. Lecture Notes in Computer Science, 2019, , 473-502.	1.0	18
7	Building an Efficient Lattice Gadget Toolkit: Subgaussian Sampling and More. Lecture Notes in Computer Science, 2019, , 655-684.	1.0	17
8	Symbolic Encryption with Pseudorandom Keys. Lecture Notes in Computer Science, 2019, , 64-93.	1.0	0
9	Faster Gaussian Sampling for Trapdoor Lattices with Arbitrary Modulus. Lecture Notes in Computer Science, 2018, , 174-203.	1.0	49
10	Asymptotically Efficient Lattice-Based Digital Signatures. Journal of Cryptology, 2018, 31, 774-797.	2.1	23
11	Symbolic Security of Garbled Circuits. , 2018, , .		6
12	Equational Security Proofs of Oblivious Transfer Protocols. Lecture Notes in Computer Science, 2018, , 527-553.	1.0	6
13	Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time. Lecture Notes in Computer Science, 2017, , 455-485.	1.0	53
14	Shortest Vector Problem. , 2016, , 1974-1977.		1
15	Creating Cryptographic Challenges Using Multi-Party Computation. , 2016, , .		9
16	Practical, Predictable Lattice Basis Reduction. Lecture Notes in Computer Science, 2016, , 820-849.	1.0	55
17	Compactness vs Collusion Resistance in Functional Encryption. Lecture Notes in Computer Science, 2016, , 443-468.	1.0	18
18	FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. Lecture Notes in Computer Science, 2015, , 617-640.	1.0	304

#	ARTICLE	IF	CITATIONS
19	Locally Dense Codes. , 2014, , .		8
20	Improved Short Lattice Signatures in the Standard Model. Lecture Notes in Computer Science, 2014, , 335-352.	1.0	69
21	A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computations. SIAM Journal on Computing, 2013, 42, 1364-1391.	0.8	75
22	An equational approach to secure multi-party computation. , 2013, , .		11
23	Hardness of SIS and LWE with Small Parameters. Lecture Notes in Computer Science, 2013, , 21-39.	1.0	158
24	Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Lecture Notes in Computer Science, 2012, , 700-718.	1.0	660
25	Title is missing!. Theory of Computing, 2012, 8, 487-512.	0.3	30
26	The Geometry of Lattice Cryptography. Lecture Notes in Computer Science, 2011, , 185-210.	1.0	5
27	Closest Vector Problem. , 2011, , 212-214.		2
28	Lattice-Based Cryptography. , 2011, , 713-715.		48
29	Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions. Lecture Notes in Computer Science, 2011, , 465-484.	1.0	104
30	The RSA Group is Pseudo-Free. Journal of Cryptology, 2010, 23, 169-186.	2.1	12
31	A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. , 2010, , .		118
32	A first glimpse of cryptography's Holy Grail. Communications of the ACM, 2010, 53, 96-96.	3.3	53
33	Computational Soundness, Co-induction, and Encryption Cycles. Lecture Notes in Computer Science, 2010, , 362-380.	1.0	5
34	Lattice-based Cryptography. , 2009, , 147-191.		349
35	Cryptographic Functions from Worst-Case Complexity Assumptions. Information Security and Cryptography, 2009, , 427-452.	0.2	6
36	On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem. Lecture Notes in Computer Science, 2009, , 577-594.	1.0	70

#	ARTICLE	IF	CITATIONS
37	Optimal Communication Complexity of Generic Multicast Key Distribution. <i>IEEE/ACM Transactions on Networking</i> , 2008, 16, 803-813.	2.6	18
38	Efficient bounded distance decoders for Barnes-Wall lattices. , 2008, , .		13
39	An Indistinguishability-Based Characterization of Anonymous Channels. <i>Lecture Notes in Computer Science</i> , 2008, , 24-43.	1.0	28
40	SWIFFT: A Modest Proposal for FFT Hashing. <i>Lecture Notes in Computer Science</i> , 2008, , 54-72.	1.0	151
41	Asymptotically Efficient Lattice-Based Digital Signatures. , 2008, , 37-54.		96
42	Shortest Vector Problem. , 2008, , 841-843.		0
43	The Round-Complexity of Black-Box Zero-Knowledge: A Combinatorial Characterization. , 2008, , 535-552.		1
44	Worst-Case to Average-Case Reductions Based on Gaussian Measures. <i>SIAM Journal on Computing</i> , 2007, 37, 267-302.	0.8	545
45	Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions. <i>Computational Complexity</i> , 2007, 16, 365-411.	0.2	164
46	On Bounded Distance Decoding for General Lattices. <i>Lecture Notes in Computer Science</i> , 2006, , 450-461.	1.0	23
47	Concurrent Zero Knowledge Without Complexity Assumptions. <i>Lecture Notes in Computer Science</i> , 2006, , 1-20.	1.0	20
48	Generalized Compact Knapsacks Are Collision Resistant. <i>Lecture Notes in Computer Science</i> , 2006, , 144-155.	1.0	195
49	Corrupting One vs. Corrupting Many: The Case of Broadcast and Multicast Encryption. <i>Lecture Notes in Computer Science</i> , 2006, , 70-82.	1.0	15
50	The complexity of the covering radius problem. <i>Computational Complexity</i> , 2005, 14, 90-121.	0.2	40
51	The RSA Group is Pseudo-Free. <i>Lecture Notes in Computer Science</i> , 2005, , 387-403.	1.0	8
52	Simultaneous broadcast revisited. , 2005, , .		8
53	LATTICE BASED CRYPTOGRAPHY. , 2005, , 347-349.		3
54	Adaptive Security of Symbolic Encryption. <i>Lecture Notes in Computer Science</i> , 2005, , 169-187.	1.0	29

#	ARTICLE	IF	CITATIONS
55	Closest Vector Problem. , 2005, , 79-80.		1
56	Shortest Vector Problem. , 2005, , 569-570.		1
57	Completeness theorems for the Abadiâ€™Rogaway language of encrypted expressions1. Journal of Computer Security, 2004, 12, 99-129.	0.5	55
58	Almost Perfect Lattices, the Covering Radius Problem, and Applications to Ajtai's Connection Factor. SIAM Journal on Computing, 2004, 34, 118-169.	0.8	54
59	The inapproximability of lattice and coding problems with preprocessing. Journal of Computer and System Sciences, 2004, 69, 45-67.	0.9	37
60	Soundness of Formal Encryption in the Presence of Active Adversaries. Lecture Notes in Computer Science, 2004, , 133-151.	1.0	123
61	Optimal Communication Complexity of Generic Multicast Key Distribution. Lecture Notes in Computer Science, 2004, , 153-170.	1.0	25
62	Simulatable Commitments and Efficient Concurrent Zero-Knowledge. Lecture Notes in Computer Science, 2003, , 140-159.	1.0	17
63	Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More. Lecture Notes in Computer Science, 2003, , 282-298.	1.0	92
64	Efficient Generic Forward-Secure Signatures with an Unbounded Number of Time Periods. Lecture Notes in Computer Science, 2002, , 400-417.	1.0	83
65	A Note on the Minimal Volume of Almost Cubic Parallelepipeds. Discrete and Computational Geometry, 2002, 29, 133-138.	0.4	2
66	The Provable Security of Graph-Based One-Time Signatures and Extensions to Algebraic Signature Schemes. Lecture Notes in Computer Science, 2002, , 379-396.	1.0	24
67	Cryptanalysis of a Pseudorandom Generator Based on Braid Groups. Lecture Notes in Computer Science, 2002, , 1-13.	1.0	7
68	Complexity of Lattice Problems. , 2002, , .		345
69	Closest Vector Problem. , 2002, , 45-68.		6
70	Cryptographic Functions. , 2002, , 143-194.		22
71	Basis Reduction Problems. , 2002, , 125-142.		1
72	Interactive Proof Systems. , 2002, , 195-210.		0

#	ARTICLE	IF	CITATIONS
73	Shortest Vector Problem. , 2002, , 69-90.		2
74	Sphere Packings. , 2002, , 91-110.		0
75	A linear space algorithm for computing the hermite normal form. , 2001, , .		30
76	The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant. SIAM Journal on Computing, 2001, 30, 2008-2035.	0.8	132
77	Improving Lattice Based Cryptosystems Using the Hermite Normal Form. Lecture Notes in Computer Science, 2001, , 126-145.	1.0	105
78	Perfectly one-way probabilistic hash functions (preliminary version). , 1998, , .		108
79	An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. , 1998, , .		40
80	Oblivious data structures. , 1997, , .		58
81	A New Paradigm for Collision-Free Hashing: Incrementality at Reduced Cost. Lecture Notes in Computer Science, 1997, , 163-192.	1.0	114
82	An algorithm for the solution of tree equations. Lecture Notes in Computer Science, 1997, , 417-428.	1.0	1