Damien StehlÃ©

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11837428/publications.pdf

Version: 2024-02-01

21	1,344	759233 12	888059 17
papers	citations	h-index	g-index

21	21	21	552
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Classical hardness of learning with errors. , 2013, , .		368
2	Worst-case to average-case reductions for module lattices. Designs, Codes, and Cryptography, 2015, 75, 565-599.	1.6	287
3	Semantically Secure Lattice Codes for the Gaussian Wiretap Channel. IEEE Transactions on Information Theory, 2014, 60, 6399-6416.	2.4	116
4	An LLL Algorithm with Quadratic Complexity. SIAM Journal on Computing, 2009, 39, 874-903.	1.0	90
5	GGHLite: More Efficient Multilinear Maps from Ideal Lattices. Lecture Notes in Computer Science, 2014, , 239-256.	1.3	84
6	Analyzing Blockwise Lattice Algorithms Using Dynamical Systems. Lecture Notes in Computer Science, 2011, , 447-464.	1.3	66
7	Decoding by Sampling: A Randomized Lattice Algorithm for Bounded Distance Decoding. IEEE Transactions on Information Theory, 2011, 57, 5933-5945.	2.4	52
8	Improved Security Proofs in Lattice-Based Cryptography: Using the RÃ©nyi Divergence Rather Than the Statistical Distance. Lecture Notes in Computer Science, 2015, , 3-24.	1.3	51
9	On the Ring-LWE and Polynomial-LWE Problems. Lecture Notes in Computer Science, 2018, , 146-173.	1.3	40
10	Improved Security Proofs in Lattice-Based Cryptography: Using the RÃ©nyi Divergence Rather than the Statistical Distance. Journal of Cryptology, 2018, 31, 610-640.	2.8	39
11	An LLL-reduction algorithm with quasi-linear time complexity. , 2011, , .		35
12	Hardness of k-LWE and Applications in Traitor Tracing. Lecture Notes in Computer Science, 2014, , 315-334.	1.3	30
13	Approx-SVP in Ideal Lattices with Pre-processing. Lecture Notes in Computer Science, 2019, , 685-716.	1.3	24
14	On the Hardness of the NTRU Problem. Lecture Notes in Computer Science, 2021, , 3-35.	1.3	18
15	Floating-Point LLL: Theoretical and Practical Aspects. Information Security and Cryptography, 2009, , 179-213.	0.3	12
16	An LLL Algorithm for Module Lattices. Lecture Notes in Computer Science, 2019, , 59-90.	1.3	12
17	Faster LLL-type Reduction of Lattice Bases. , 2016, , .		10
18	MPSign: A Signature from Small-Secret Middle-Product Learning with Errors. Lecture Notes in Computer Science, 2020, , 66-93.	1.3	5

#	Article	IF	Citations
19	Lattice Reduction Algorithms. , 2017, , .		3
20	On the Integer Polynomial Learning with Errors Problem. Lecture Notes in Computer Science, 2021, , 184-214.	1.3	1
21	Towards Practical GGM-Based PRF from (Module-)Learning-with-Rounding. Lecture Notes in Computer Science, 2020, , 693-713.	1.3	1