Chris Peikert

List of Publications by Year
in descending order

21 papers	4,874 citations	516710 16 h-index	888059 17 g-index
21 all docs	21 docs citations	21 times ranked	1144 citing authors

#	Article	IF	Citations
1	Trapdoors for hard lattices and new cryptographic constructions. , 2008, , .		1,315
2	Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Lecture Notes in Computer Science, 2012, , 700-718.	1.3	660
3	Public-key cryptosystems from the worst-case shortest vector problem. , 2009, , .		504
4	Bonsai Trees, or How to Delegate a Lattice Basis. Lecture Notes in Computer Science, 2010, , 523-552.	1.3	436
5	A Framework for Efficient and Composable Oblivious Transfer. Lecture Notes in Computer Science, 2008, , 554-571.	1.3	402
6	A Decade of Lattice Cryptography. Foundations and Trends in Theoretical Computer Science, 2016, 10, 283-424.	0.3	241
7	Generating Shorter Bases for Hard Random Lattices. Theory of Computing Systems, 2011, 48, 535-553.	1.1	226
8	A Toolkit for Ring-LWE Cryptography. Lecture Notes in Computer Science, 2013, , 35-54.	1.3	223
9	Lattice Cryptography for the Internet. Lecture Notes in Computer Science, 2014, , 197-219.	1.3	207
10	Bonsai Trees, or How to Delegate a Lattice Basis. Journal of Cryptology, 2012, 25, 601-639.	2.8	146
11	Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors. Lecture Notes in Computer Science, 2019, , 89-114.	1.3	123
12	Lossy Trapdoor Functions and Their Applications. SIAM Journal on Computing, 2011, 40, 1803-1844.	1.0	107
13	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. Journal of Cryptology, 2015, 28, 820-843.	2.8	50
14	Limits on the Hardness of Lattice Problems in â„“ p Norms. Computational Complexity, 2008, 17, 300-351.	0.3	44
15	Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems. Lecture Notes in Computer Science, 2008, , 536-553.	1.3	43
16	Identity-Based (Lossy) Trapdoor Functions and Applications. Lecture Notes in Computer Science, 2012, , 228-245.	1.3	41
17	How to Share a Lattice Trapdoor: Threshold Protocols for Signatures and (H)IBE. Lecture Notes in Computer Science, 2013, , 218-236.	1.3	33
18	ALCHEMY. , 2018, , .		28

#	Article	IF	Citations
19	Algebraically Structured LWE, Revisited. Lecture Notes in Computer Science, 2019, , 1-23.	1.3	18
20	On the Lattice Smoothing Parameter Problem. , 2013, , .		14
21	Vector and Functional Commitments from Lattices. Lecture Notes in Computer Science, 2021, , 480-511.	1.3	13