Chris Peikert

List of Publications by Year
in descending order

21 papers	**4,874** citations	586496 **16** h-index	993246 **17** g-index
21 all docs	**21** docs citations	**21** times ranked	**1255** citing authors

#	Article	IF	Citations
1	Vector and Functional Commitments from Lattices. Lecture Notes in Computer Science, 2021, , 480-511.	1.0	13
2	Noninteractive Zero Knowledge for NP from (Plain) Learning with Errors. Lecture Notes in Computer Science, 2019, , 89-114.	1.0	123
3	Algebraically Structured LWE, Revisited. Lecture Notes in Computer Science, 2019, , 1-23.	1.0	18
4	ALCHEMY. , 2018, , .		28
5	A Decade of Lattice Cryptography. Foundations and Trends in Theoretical Computer Science, 2016, 10, 283-424.	2.0	241
6	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. Journal of Cryptology, 2015, 28, 820-843.	2.1	50
7	Lattice Cryptography for the Internet. Lecture Notes in Computer Science, 2014, , 197-219.	1.0	207
8	On the Lattice Smoothing Parameter Problem. , 2013, , .		14
9	A Toolkit for Ring-LWE Cryptography. Lecture Notes in Computer Science, 2013, , 35-54.	1.0	223
10	How to Share a Lattice Trapdoor: Threshold Protocols for Signatures and (H)IBE. Lecture Notes in Computer Science, 2013, , 218-236.	1.0	33
11	Bonsai Trees, or How to Delegate a Lattice Basis. Journal of Cryptology, 2012, 25, 601-639.	2.1	146
12	Identity-Based (Lossy) Trapdoor Functions and Applications. Lecture Notes in Computer Science, 2012, , 228-245.	1.0	41
13	Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Lecture Notes in Computer Science, 2012, , 700-718.	1.0	660
14	Lossy Trapdoor Functions and Their Applications. SIAM Journal on Computing, 2011, 40, 1803-1844.	0.8	107
15	Generating Shorter Bases for Hard Random Lattices. Theory of Computing Systems, 2011, 48, 535-553.	0.7	226
16	Bonsai Trees, or How to Delegate a Lattice Basis. Lecture Notes in Computer Science, 2010, , 523-552.	1.0	436
17	Public-key cryptosystems from the worst-case shortest vector problem. , 2009, , .		504
18	Limits on the Hardness of Lattice Problems in ℓ_p Norms. Computational Complexity, 2008, 17, 300-351.	0.2	44

#	ARTICLE	IF	CITATIONS
19	Trapdoors for hard lattices and new cryptographic constructions. , 2008, , .		1,315
20	Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems. Lecture Notes in Computer Science, 2008, , 536-553.	1.0	43
21	A Framework for Efficient and Composable Oblivious Transfer. Lecture Notes in Computer Science, 2008, , 554-571.	1.0	402