Adam Smith

List of Publications by Year
in descending order

		858243		1113639
24 papers	5,955 citations	12 h-index		15 g-index
25 all docs	25 docs citations	25 times ranked		3742 citing authors

#	Article	IF	Citations
1	Reusable Fuzzy Extractors for Low-Entropy Distributions. Journal of Cryptology, 2021, 34, 1.	2.1	24
2	When is memorization of irrelevant training data necessary for high-accuracy learning?. , 2021, , .		14
3	When Are Fuzzy Extractors Possible?. IEEE Transactions on Information Theory, 2020, 66, 5282-5298.	1.5	13
4	When is non-trivial estimation possible for graphons and stochastic block models?â€¡. Information and Inference, 2018, 7, 169-181.	0.9	0
5	Exposed! A Survey of Attacks on Private Data. Annual Review of Statistics and Its Application, 2017, 4, 61-84.	4.1	103
6	Lipschitz Extensions for Node-Private Graph Statistics and the Generalized Exponential Mechanism. , 2016, , .		17
7	Max-Information, Differential Privacy, and Post-selection Hypothesis Testing. , 2016, , .		14
8	Robust Traceability from Trace Amounts. , 2015, , .		52
9	Classical cryptographic protocols in a quantum world. International Journal of Quantum Information, 2015, 13, 1550028.	0.6	7
10	Private Analysis of Graph Structure. ACM Transactions on Database Systems, 2014, 39, 1-33.	1.5	60
11	Sublinear Algorithms for Approximating String Compressibility. Algorithmica, 2013, 65, 685-709.	1.0	22
12	Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IEEE Transactions on Information Theory, 2012, 58, 6207-6222.	1.5	63
13	Leftover Hashing Against Quantum Side Information. IEEE Transactions on Information Theory, 2011, 57, 5524-5535.	1.5	213
14	Private analysis of graph structure. Proceedings of the VLDB Endowment, 2011, 4, 1146-1157.	2.1	87
15	Parallel and Concurrent Security of the HB and HB+ Protocols. Journal of Cryptology, 2010, 23, 402-421.	2.1	64
16	Codes for Computationally Simple Channels: Explicit Constructions with Optimal Rate. , 2010, , .		46
17	Strong Lower Bounds for Approximating Distribution Support Size and the Distinct Elements Problem. SIAM Journal on Computing, 2009, 39, 813-842.	0.8	52
18	Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. IEEE Transactions on Information Theory, 2008, 54, 2408-2425.	1.5	10

#	Article	IF	Citations
19	Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 2008, 38, 97-139.	0.8	1,172
20	Defending Against Attacks on Main Memory Persistence. , 2008, , .		24
21	What Can We Learn Privately?. , 2008, , .		200
22	Smooth sensitivity and sampling in private data analysis. , 2007, , .		528
23	Correcting errors without leaking partial information. , 2005, , .		100
24	Efficient and Non-interactive Non-malleable Commitment. Lecture Notes in Computer Science, 2001, , 40-59.	1.0	76