

Adam Smith

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/10898536/publications.pdf>

Version: 2024-02-01

24
papers

5,955
citations

759233

12
h-index

996975

15
g-index

25
all docs

25
docs citations

25
times ranked

3320
citing authors

#	ARTICLE	IF	CITATIONS
1	Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 2008, 38, 97-139.	1.0	1,172
2	Smooth sensitivity and sampling in private data analysis. , 2007, , .		528
3	Leftover Hashing Against Quantum Side Information. IEEE Transactions on Information Theory, 2011, 57, 5524-5535.	2.4	213
4	What Can We Learn Privately?. , 2008, , .		200
5	Exposed! A Survey of Attacks on Private Data. Annual Review of Statistics and Its Application, 2017, 4, 61-84.	7.0	103
6	Correcting errors without leaking partial information. , 2005, , .		100
7	Private analysis of graph structure. Proceedings of the VLDB Endowment, 2011, 4, 1146-1157.	3.8	87
8	Efficient and Non-interactive Non-malleable Commitment. Lecture Notes in Computer Science, 2001, , 40-59.	1.3	76
9	Parallel and Concurrent Security of the HB and HB+ Protocols. Journal of Cryptology, 2010, 23, 402-421.	2.8	64
10	Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IEEE Transactions on Information Theory, 2012, 58, 6207-6222.	2.4	63
11	Private Analysis of Graph Structure. ACM Transactions on Database Systems, 2014, 39, 1-33.	2.8	60
12	Strong Lower Bounds for Approximating Distribution Support Size and the Distinct Elements Problem. SIAM Journal on Computing, 2009, 39, 813-842.	1.0	52
13	Robust Traceability from Trace Amounts. , 2015, , .		52
14	Codes for Computationally Simple Channels: Explicit Constructions with Optimal Rate. , 2010, , .		46
15	Defending Against Attacks on Main Memory Persistence. , 2008, , .		24
16	Reusable Fuzzy Extractors for Low-Entropy Distributions. Journal of Cryptology, 2021, 34, 1.	2.8	24
17	Sublinear Algorithms for Approximating String Compressibility. Algorithmica, 2013, 65, 685-709.	1.3	22
18	Lipschitz Extensions for Node-Private Graph Statistics and the Generalized Exponential Mechanism. , 2016, , .		17

#	ARTICLE	IF	CITATIONS
19	Max-Information, Differential Privacy, and Post-selection Hypothesis Testing. , 2016, , .		14
20	When is memorization of irrelevant training data necessary for high-accuracy learning?. , 2021, , .		14
21	When Are Fuzzy Extractors Possible?. IEEE Transactions on Information Theory, 2020, 66, 5282-5298.	2.4	13
22	Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. IEEE Transactions on Information Theory, 2008, 54, 2408-2425.	2.4	10
23	Classical cryptographic protocols in a quantum world. International Journal of Quantum Information, 2015, 13, 1550028.	1.1	7
24	When is non-trivial estimation possible for graphons and stochastic block models?â€¦. Information and Inference, 2018, 7, 169-181.	1.6	0