Dana Dachman-Soled

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/12107391/publications.pdf

Version: 2024-02-01

13 papers	234 citations	1478505 6 h-index	1281871 11 g-index
13 all docs	13 docs citations	13 times ranked	94 citing authors

#	Article	IF	Citations
1	Efficient Robust Private Set Intersection. Lecture Notes in Computer Science, 2009, , 125-142.	1.3	101
2	Non-malleable Codes for Bounded Depth, Bounded Fan-In Circuits. Lecture Notes in Computer Science, 2016, , 881-908.	1.3	38
3	Adaptively Secure, Universally Composable, Multiparty Computation in Constant Rounds. Lecture Notes in Computer Science, 2015, , 586-613.	1.3	31
4	Non-Malleable Codes for Small-Depth Circuits. , 2018, , .		21
5	A Black-Box Construction of Non-malleable Encryption from Semantically Secure Encryption. Journal of Cryptology, 2018, 31, 172-201.	2.8	9
6	Securing Circuits and Protocols against 1/poly(k) Tampering Rate. Lecture Notes in Computer Science, 2014, , 540-565.	1.3	9
7	A Black-Box Construction of a CCA2 Encryption Scheme from a Plaintext Aware (sPA1) Encryption Scheme. Lecture Notes in Computer Science, 2014, , 37-55.	1.3	8
8	Locally Decodable and Updatable Non-malleable Codes and Their Applications. Journal of Cryptology, 2020, 33, 319-355.	2.8	6
9	Improved, black-box, non-malleable encryption from semantic security. Designs, Codes, and Cryptography, 2018, 86, 641-663.	1.6	4
10	Leakage Resilience from Program Obfuscation. Journal of Cryptology, 2019, 32, 742-824.	2.8	3
11	(In)Security of Ring-LWE Under Partial Key Exposure. Journal of Mathematical Cryptology, 2020, 15, 72-86.	0.7	2
12	Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness. Journal of Cryptology, 2019, 32, 941-972.	2.8	1
13	Towards a Ring Analogue of the Leftover Hash Lemma. Journal of Mathematical Cryptology, 2020, 15, 87-110.	0.7	1