

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