Eran Tromer

List of Publications by Year
in descending order

12 papers	2,245 citations	933447 10 h-index	1372567 10 g-index
13 all docs	13 docs citations	13 times ranked	1023 citing authors

#	Article	IF	Citations
1	Efficient Cache Attacks on AES, and Countermeasures. Journal of Cryptology, 2010, 23, 37-71.	2.8	325
2	SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge. Lecture Notes in Computer Science, 2013, , 90-108.	1.3	304
3	From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. , 2012, , .		255
4	RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Lecture Notes in Computer Science, 2014, , 444-461.	1.3	182
5	Recursive composition and bootstrapping for SNARKS and proof-carrying data. , 2013, , .		164
6	Scalable Zero Knowledge via Cycles of Elliptic Curves. Lecture Notes in Computer Science, 2014, , 276-294.	1.3	86
7	Get your hands off my laptop: physical side-channel key-extraction attacks on PCs. Journal of Cryptographic Engineering, 2015, 5, 95-112.	1.8	67
8	Acoustic Cryptanalysis. Journal of Cryptology, 2017, 30, 392-443.	2.8	60
9	Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs. Lecture Notes in Computer Science, 2014, , 242-260.	1.3	52
10	The Hunting of the SNARK. Journal of Cryptology, 2017, 30, 989-1066.	2.8	51
11	On the concrete efficiency of probabilistically-checkable proofs. , 2013, , .		44
12	Drive-By Key-Extraction Cache Attacks from Portable Code. Lecture Notes in Computer Science, 2018, , 83-102.	1.3	21