Sourav Sengupta

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4405474/publications.pdf

Version: 2024-02-01

22 papers	382 citations	1163117 8 h-index	996975 15 g-index
24 all docs	24 docs citations	24 times ranked	250 citing authors

#	Article	IF	Citations
1	A Blockchain Framework for Insurance Processes. , 2018, , .		97
2	High-Performance Hardware Implementation for RC4 Stream Cipher. IEEE Transactions on Computers, 2013, 62, 730-743.	3.4	50
3	(Non-)Random Sequences from (Non-)Random Permutationsâ€"Analysis of RC4 Stream Cipher. Journal of Cryptology, 2014, 27, 67-108.	2.8	48
4	Measurements, Analyses, and Insights on the Entire Ethereum Blockchain Network. , 2020, , .		48
5	Attack on Broadcast RC4 Revisited. Lecture Notes in Computer Science, 2011, , 199-217.	1.3	26
6	Designing integrated accelerator for stream ciphers with structural similarities. Cryptography and Communications, 2013, 5, 19-47.	1.4	23
7	Security is an architectural design constraint. Microprocessors and Microsystems, 2019, 68, 17-27.	2.8	8
8	HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers. Lecture Notes in Computer Science, 2011, , 196-215.	1.3	8
9	Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. Lecture Notes in Computer Science, 2015, , 350-369.	1.3	8
10	Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles. , 2018, , .		7
11	Curse of Dimensionality in Adversarial Examples. , 2019, , .		6
12	Factoring RSA Modulus Using Prime Reconstruction from Random Known Bits. Lecture Notes in Computer Science, 2010, , 82-99.	1.3	6
13	Proving TLS-attack related open biases of RC4. Designs, Codes, and Cryptography, 2015, 77, 231-253.	1.6	5
14	One Byte per Clock: A Novel RC4 Hardware. Lecture Notes in Computer Science, 2010, , 347-363.	1.3	5
15	New Long-Term Glimpse of RC4 Stream Cipher. Lecture Notes in Computer Science, 2013, , 230-238.	1.3	4
16	COUNTING HERON TRIANGLES WITH CONSTRAINTS. , 2014, , 24-40.		2
17	Improving Speed of Dilithiumâ€™s Signing Procedure. Lecture Notes in Computer Science, 2020, , 57-73.	1.3	2
18	Publishing Upper Half of RSA Decryption Exponent. Lecture Notes in Computer Science, 2010, , 25-39.	1.3	1

#	Article	IF	Citations
19	Error Correction of Partially Exposed RSA Private Keys from MSB Side. Lecture Notes in Computer Science, 2013, , 345-359.	1.3	1
20	Parallelized Common Factor Attack on RSA. Lecture Notes in Computer Science, 2017, , 303-312.	1.3	0
21	On Random Read Access in ${mathsf{OCB}}$. IEEE Transactions on Information Theory, 2019, 65, 8325-8344.	2.4	0
22	Traitor-Traceable Key Pre-distribution Based on Visual Secret Sharing. Lecture Notes in Computer Science, 2013, , 199-213.	1.3	0