

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	Measurements, Analyses, and Insights on the Entire Ethereum Blockchain Network. , 2020, , .		48
2	Improving Speed of Dilithium™s Signing Procedure. Lecture Notes in Computer Science, 2020, , 57-73.	1.3	2
3	On Random Read Access in \mathcal{OCB} . IEEE Transactions on Information Theory, 2019, 65, 8325-8344.	2.4	0
4	Security is an architectural design constraint. Microprocessors and Microsystems, 2019, 68, 17-27.	2.8	8
5	Curse of Dimensionality in Adversarial Examples. , 2019, , .		6
6	A Blockchain Framework for Insurance Processes. , 2018, , .		97
7	Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles. , 2018, , .		7
8	Parallelized Common Factor Attack on RSA. Lecture Notes in Computer Science, 2017, , 303-312.	1.3	0
9	Proving TLS-attack related open biases of RC4. Designs, Codes, and Cryptography, 2015, 77, 231-253.	1.6	5
10	Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. Lecture Notes in Computer Science, 2015, , 350-369.	1.3	8
11	(Non-)Random Sequences from (Non-)Random Permutationsâ€”Analysis of RC4 Stream Cipher. Journal of Cryptology, 2014, 27, 67-108.	2.8	48
12	COUNTING HERON TRIANGLES WITH CONSTRAINTS. , 2014, , 24-40.		2
13	Designing integrated accelerator for stream ciphers with structural similarities. Cryptography and Communications, 2013, 5, 19-47.	1.4	23
14	High-Performance Hardware Implementation for RC4 Stream Cipher. IEEE Transactions on Computers, 2013, 62, 730-743.	3.4	50
15	New Long-Term Glimpse of RC4 Stream Cipher. Lecture Notes in Computer Science, 2013, , 230-238.	1.3	4
16	Error Correction of Partially Exposed RSA Private Keys from MSB Side. Lecture Notes in Computer Science, 2013, , 345-359.	1.3	1
17	Traitor-Traceable Key Pre-distribution Based on Visual Secret Sharing. Lecture Notes in Computer Science, 2013, , 199-213.	1.3	0
18	Attack on Broadcast RC4 Revisited. Lecture Notes in Computer Science, 2011, , 199-217.	1.3	26

#	ARTICLE	IF	CITATIONS
19	HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers. Lecture Notes in Computer Science, 2011, , 196-215.	1.3	8
20	Factoring RSA Modulus Using Prime Reconstruction from Random Known Bits. Lecture Notes in Computer Science, 2010, , 82-99.	1.3	6
21	One Byte per Clock: A Novel RC4 Hardware. Lecture Notes in Computer Science, 2010, , 347-363.	1.3	5
22	Publishing Upper Half of RSA Decryption Exponent. Lecture Notes in Computer Science, 2010, , 25-39.	1.3	1