Somitra Kumar Sanadhya

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7682037/publications.pdf

Version: 2024-02-01

45	376	932766	887659
papers	citations	10 h-index	17 g-index

46	46	46	252
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	FPGA-Based True Random Number Generation Using Programmable Delays in Oscillator-Rings. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67, 570-574.	2.2	58
2	New Collision Attacks against Up to 24-Step SHA-2. Lecture Notes in Computer Science, 2008, , 91-103.	1.0	41
3	Compact Implementations of FPGA-based PUFs with Enhanced Performance. , 2017, , .		24
4	Cryptanalysis of SIMON Variants with Connections. Lecture Notes in Computer Science, 2014, , 90-107.	1.0	22
5	Differential Fault Analysis of SHA-3. Lecture Notes in Computer Science, 2015, , 253-269.	1.0	18
6	FbHash: A New Similarity Hashing Scheme for Digital Forensics. Digital Investigation, 2019, 29, S113-S123.	3.2	17
7	Threshold Implementations of $mathtt{GIFT}$: A Trade-Off Analysis. IEEE Transactions on Information Forensics and Security, 2020, 15, 2110-2120.	4.5	16
8	Efficient and Lightweight FPGA-based Hybrid PUFs with Improved Performance. Microprocessors and Microsystems, 2020, 77, 103180.	1.8	15
9	Design and Analysis of FPGA-based PUFs with Enhanced Performance for Hardware-oriented Security. ACM Journal on Emerging Technologies in Computing Systems, 2022, 18, 1-26.	1.8	13
10	Attacking Reduced Round SHA-256. Lecture Notes in Computer Science, 2008, , 130-143.	1.0	11
11	Non-linear Reduced Round Attacks against SHA-2 Hash Family. Lecture Notes in Computer Science, 2008, , 254-266.	1.0	10
12	Generation of Secure and Reliable Honeywords, Preventing False Detection. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 757-769.	3.7	10
13	Bicliques with Minimal Data and Time Complexity for AES. Lecture Notes in Computer Science, 2015, , 160-174.	1.0	10
14	New Local Collisions for the SHA-2 Hash Family. , 2007, , 193-205.		9
15	Quantum Resource Estimates of Groverâ€™s Key Search on ARIA. Lecture Notes in Computer Science, 2020, , 238-258.	1.0	9
16	Field Programmable Gate Array based elliptic curve Menezesâ€Quâ€Vanstone key agreement protocol realization using Physical Unclonable Function and true random number generator primitives. IET Circuits, Devices and Systems, 2022, 16, 382-398.	0.9	9
17	Improved Meet-in-the-Middle Attacks on 7 and 8-Round ARIA-192 and ARIA-256. Lecture Notes in Computer Science, 2015, , 198-217.	1.0	7
18	Design, Implementation and Analysis of Efficient Hardware-Based Security Primitives. , 2020, , .		7

#	Article	IF	Citations
19	A new authenticated encryption technique for handling long ciphertexts in memory constrained devices. International Journal of Applied Cryptography, 2017, 3, 236.	0.4	5
20	RCB: leakage-resilient authenticated encryption via re-keying. Journal of Supercomputing, 2018, 74, 4173-4198.	2.4	5
21	Cryptanalytic timeâ€“memory trade-off for password hashing schemes. International Journal of Information Security, 2019, 18, 163-180.	2.3	5
22	Sponge Based CCA2 Secure Asymmetric Encryption for Arbitrary Length Message. Lecture Notes in Computer Science, 2015, , 93-106.	1.0	5
23	SPF: A New Family of Efficient Format-Preserving Encryption Algorithms. Lecture Notes in Computer Science, 2017, , 64-83.	1.0	5
24	On the Security of Two RFID Mutual Authentication Protocols. Lecture Notes in Computer Science, 2013, , 86-99.	1.0	5
25	On identifying marker genes from gene expression data in a neural framework through online feature analysis. International Journal of Intelligent Systems, 2006, 21, 453-467.	3.3	4
26	Revocable Identity-Based Encryption from Codes with Rank Metric. Lecture Notes in Computer Science, 2018, , 435-451.	1.0	4
27	Rig: A Simple, Secure and Flexible Design for Password Hashing. Lecture Notes in Computer Science, 2015, , 361-381.	1.0	4
28	On the Security of Mutual Authentication Protocols for RFID Systems: The Case of Wei et al.â€™s Protocol. Lecture Notes in Computer Science, 2012, , 90-103.	1.0	3
29	eSPF: A Family of Format-Preserving Encryption Algorithms Using MDS Matrices. Lecture Notes in Computer Science, 2017, , 133-150.	1.0	3
30	Deterministic Constructions of 21-Step Collisions for the SHA-2 Hash Family. Lecture Notes in Computer Science, 2008, , 244-259.	1.0	3
31	PPAE: Practical Parazoa Authenticated Encryption Family. Lecture Notes in Computer Science, 2015, , 198-211.	1.0	2
32	Exploiting the Leakage: Analysis of Some Authenticated Encryption Schemes. Lecture Notes in Computer Science, 2016, , 383-401.	1.0	2
33	Distinguishers for 4-Branch and 8-Branch Generalized Feistel Network. IEEE Access, 2017, 5, 27857-27867.	2.6	2
34	Single Key Recovery Attacks on 9-Round Kalyna-128/256 and Kalyna-256/512. Lecture Notes in Computer Science, 2016, , 119-135.	1.0	2
35	A new hash family obtained by modifying the SHA-2 family. , 2009, , .		1
36	A combinatorial analysis of recent attacks on step reduced SHA-2 family. Cryptography and Communications, 2009, 1, 135-173.	0.9	1

#	Article	IF	Citations
37	Sponge-based CCA2 secure asymmetric encryption for arbitrary length message (extended version). International Journal of Applied Cryptography, 2017, 3, 262.	0.4	1
38	A Generalized Format Preserving Encryption Framework Using MDS Matrices. Journal of Hardware and Systems Security, 2019, 3, 3-11.	0.8	1
39	Collision Attack on 4-Branch, Type-2 GFN Based Hash Functions Using Sliced Biclique Cryptanalysis Technique. Lecture Notes in Computer Science, 2015, , 343-360.	1.0	1
40	Biclique Cryptanalysis of Full Round AES-128 Based Hashing Modes. Lecture Notes in Computer Science, 2016, , 3-21.	1.0	1
41	Desynchronization and Traceability Attacks on RIPTA-DA Protocol. Lecture Notes in Computer Science, 2013, , 57-68.	1.0	1
42	Counting Active S-Boxes is not Enough. Lecture Notes in Computer Science, 2020, , 332-344.	1.0	1
43	FbHash-E: A time and memory efficient version of FbHash similarity hashing algorithm. Forensic Science International: Digital Investigation, 2022, 41, 301375.	1.2	1
44	New HMAC Message Patches: Secret Patch and CrOw Patch. Lecture Notes in Computer Science, 2015, , 285-302.	1.0	0
45	Cryptographic Module Based Approach for Password Hashing Schemes. Lecture Notes in Computer Science, 2015, , 39-57.	1.0	0