Subhadeep Banik

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/626950/publications.pdf

Version: 2024-02-01

55	1,001	566801 15	454577 30
papers	citations	h-index	g-index

60	60	60	459
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	GIFT: A Small Present. Lecture Notes in Computer Science, 2017, , 321-345.	1.0	221
2	Midori: A Block Cipher for Low Energy. Lecture Notes in Computer Science, 2015, , 411-436.	1.0	221
3	A Differential Fault Attack on the Grain Family of Stream Ciphers. Lecture Notes in Computer Science, 2012, , 122-139.	1.0	49
4	Differential Fault Attack against Grain Family with Very Few Faults and Minimal Assumptions. IEEE Transactions on Computers, 2015, 64, 1647-1657.	2.4	32
5	Exploring Energy Efficiency of Lightweight Block Ciphers. Lecture Notes in Computer Science, 2016, , 178-194.	1.0	31
6	A Differential Fault Attack on the Grain Family under Reasonable Assumptions. Lecture Notes in Computer Science, 2012, , 191-208.	1.0	23
7	A Differential Fault Attack on MICKEY 2.0. Lecture Notes in Computer Science, 2013, , 215-232.	1.0	23
8	A Chosen IV Related Key Attack on Grain-128a. Lecture Notes in Computer Science, 2013, , 13-26.	1.0	19
9	Some Results on Sprout. Lecture Notes in Computer Science, 2015, , 124-139.	1.0	19
10	Improved differential fault attack on MICKEY 2.0. Journal of Cryptographic Engineering, 2015, 5, 13-29.	1.5	18
11	Atomic-AES: A Compact Implementation of the AES Encryption/Decryption Core. Lecture Notes in Computer Science, 2016, , 173-190.	1.0	17
12	A Differential Fault Attack on Grain-128a Using MACs. Lecture Notes in Computer Science, 2012, , 111-125.	1.0	17
13	Related-Key Impossible-Differential Attack onÂReduced-Round Skinny. Lecture Notes in Computer Science, 2017, , 208-228.	1.0	16
14	Compact circuits for combined AES encryption/decryption. Journal of Cryptographic Engineering, 2019, 9, 69-83.	1.5	16
15	Improved Scan-Chain Based Attacks and Related Countermeasures. Lecture Notes in Computer Science, 2013, , 78-97.	1.0	15
16	WARP : Revisiting GFN for Lightweight 128-Bit Block Cipher. Lecture Notes in Computer Science, 2021, , 535-564.	1.0	15
17	More Results on Shortest Linear Programs. Lecture Notes in Computer Science, 2019, , 109-128.	1.0	15
18	Some Insights into Differential Cryptanalysis of Grain v1. Lecture Notes in Computer Science, 2014, , 34-49.	1.0	14

#	Article	IF	Citations
19	Orthros: A Low-Latency PRF. IACR Transactions on Symmetric Cryptology, 0, , 37-77.	0.0	12
20	Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013. Lecture Notes in Computer Science, 2014, , 179-196.	1.0	12
21	Conditional differential cryptanalysis of 105 round Grain v1. Cryptography and Communications, 2016, 8, 113-137.	0.9	11
22	Cryptanalysis of LowMC instances using single plaintext/ciphertext pair. IACR Transactions on Symmetric Cryptology, 0, , 130-146.	0.0	11
23	Random Walks based Image Segmentation Using Color Space Graphs. Procedia Technology, 2013, 10, 271-278.	1.1	10
24	Round gating for low energy block ciphers. , 2016, , .		10
25	A low power 1.8 V 4-bit 400-MHz flash ADC in 0.18/spl mu/ digital CMOS. , 2006, , .		9
26	Some security results of the RC4+ stream cipher. Security and Communication Networks, 2015, 8, 4061-4072.	1.0	9
27	Cryptanalysis of the Full Spritz Stream Cipher. Lecture Notes in Computer Science, 2016, , 63-77.	1.0	9
28	A Study of Persistent Fault Analysis. Lecture Notes in Computer Science, 2019, , 13-33.	1.0	9
29	Cryptanalysis of Two Fault Countermeasure Schemes. Lecture Notes in Computer Science, 2015, , 241-252.	1.0	8
30	Security Analysis of the RC4+ Stream Cipher. Lecture Notes in Computer Science, 2013, , 297-307.	1.0	8
31	Design steps for bulk micro machined single axis silicon capacitive accelerometer with optimised device dimensions. Journal of Physics: Conference Series, 2006, 34, 722-727.	0.3	7
32	Cryptanalysis of ForkAES. Lecture Notes in Computer Science, 2019, , 43-63.	1.0	7
33	Synthesis of Flexible Accelerators for Early Adoption of Ring-LWE Post-quantum Cryptography. Transactions on Embedded Computing Systems, 2020, 19, 1-17.	2.1	7
34	Energy Analysis of Lightweight AEAD Circuits. Lecture Notes in Computer Science, 2020, , 23-42.	1.0	7
35	Melting SNOW-V: improved lightweight architectures. Journal of Cryptographic Engineering, 2022, 12, 53-73.	1.5	6
36	Further Results on Efficient Implementations of Block Cipher Linear Layers. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 213-225.	0.2	6

#	Article	IF	Citations
37	New Attacks onÂLowMC Instances withÂaÂSingle Plaintext/Ciphertext Pair. Lecture Notes in Computer Science, 2021, , 303-331.	1.0	6
38	Exploring the energy consumption of lightweight blockciphers in FPGA. , 2015, , .		5
39	Low-area hardware implementations of CLOC, SILC and AES-OTR. , 2016, , .		5
40	Some Proofs of Joint Distributions of Keystream Biases in RC4. Lecture Notes in Computer Science, 2016, , 305-321.	1.0	5
41	Some Results on Related Key-IV Pairs of Grain. Lecture Notes in Computer Science, 2012, , 94-110.	1.0	5
42	How Not to Combine RC4 States. Lecture Notes in Computer Science, 2015, , 95-112.	1.0	4
43	Adaptable AES implementation with power-gating support. , 2016, , .		3
44	On Design of Robust Lightweight Stream Cipher with Short Internal State. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 99-109.	0.2	3
45	Inverse gating for low energy encryption. , 2018, , .		3
46	Efficient configurations for block ciphers with unified ENC/DEC paths. , 2017, , .		2
47	A Deeper Look at the Energy Consumption of Lightweight Block Ciphers. , 2021, , .		2
48	Atom: A Stream Cipher with Double Key Filter. IACR Transactions on Symmetric Cryptology, 0, , 5-36.	0.0	2
49	Six shades lighter: a bit-serial implementation of the AES family. Journal of Cryptographic Engineering, 2021, 11, 417-439.	1.5	2
50	A scheme for conditional access-based systems using index locations of DCT coefficients. Journal of Real-Time Image Processing, 2017, 13, 363-373.	2.2	1
51	Analysis and Improvements of the Full Spritz Stream Cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1296-1305.	0.2	1
52	Exploring Lightweight Efficiency of ForkAES. Lecture Notes in Computer Science, 2019, , 514-534.	1.0	1
53	The Area-Latency Symbiosis: Towards Improved Serial Encryption Circuits. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 239-278.	0.0	1
54	Hold Your Breath, PRIMATEs Are Lightweight. Lecture Notes in Computer Science, 2017, , 197-216.	1.0	0

#	Article	IF	Citations
55	Theoretical Understanding of Some Conditional and Joint Biases in RC4 Stream Cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1869-1879.	0.2	0