Santanu Sarkar

List of Publications by Year
in descending order

76	744	516561 16	642610 23
papers	citations	h-index	g-index

81	81	81	257
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A Differential Fault Attack on the Grain Family of Stream Ciphers. Lecture Notes in Computer Science, 2012, , 122-139.	1.0	49
2	(Non-)Random Sequences from (Non-)Random Permutationsâ€"Analysis of RC4 Stream Cipher. Journal of Cryptology, 2014, 27, 67-108.	2.1	48
3	Small secret exponent attack on RSA variant with modulus $$N=p^rq$$ N = p r q. Designs, Codes, and Cryptography, 2014, 73, 383-392.	1.0	35
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	Approximate Integer Common Divisor Problem Relates to Implicit Factorization. IEEE Transactions on Information Theory, 2011, 57, 4002-4013.	1.5	31
6	Improved analysis for reduced round Salsa and Chacha. Discrete Applied Mathematics, 2017, 227, 58-69.	0.5	30
7	A Differential Fault Attack on the Grain Family under Reasonable Assumptions. Lecture Notes in Computer Science, 2012, , 191-208.	1.0	23
8	Cryptanalysis of RSA with more than one decryption exponent. Information Processing Letters, 2010, 110, 336-340.	0.4	20
9	Revisiting Wienerâ€™s Attack â€“ New Weak Keys in RSA. Lecture Notes in Computer Science, 2008, , 228-243.	1.0	20
10	A Chosen IV Related Key Attack on Grain-128a. Lecture Notes in Computer Science, 2013, , 13-26.	1.0	19
11	Revisiting Prime Power RSA. Discrete Applied Mathematics, 2016, 203, 127-133.	0.5	19
12	Cryptanalysis of RSA with two decryption exponents. Information Processing Letters, 2010, 110, 178-181.	0.4	18
13	Improved differential fault attack on MICKEY 2.0. Journal of Cryptographic Engineering, 2015, 5, 13-29.	1.5	18
14	A Differential Fault Attack on Plantlet. IEEE Transactions on Computers, 2017, 66, 1804-1808.	2.4	18
15	A Differential Fault Attack on Grain-128a Using MACs. Lecture Notes in Computer Science, 2012, , 111-125.	1.0	17
16	Observing biases in the state: case studies with Trivium and Trivia-SC. Designs, Codes, and Cryptography, 2017, 82, 351-375.	1.0	15
17	Further results on implicit factoring in polynomial time. Advances in Mathematics of Communications, 2009, 3, 205-217.	0.4	15
18	Differential Fault Attack on Grain v1, ACORN v3 and Lizard. Lecture Notes in Computer Science, 2017, , 247-263.	1.0	13

#	Article	IF	Citations
19	Differential Fault Analysis on Tiaoxin and AEGIS Family of Ciphers. Communications in Computer and Information Science, 2016, , 74-86.	0.4	12
20	Further non-randomness in RC4, RC4A and VMPC. Cryptography and Communications, 2015, 7, 317-330.	0.9	11
21	New cube distinguishers on NFSR-based stream ciphers. Designs, Codes, and Cryptography, 2020, 88, 173-199.	1.0	11
22	Probabilistic signature based generalized framework for differential fault analysis of stream ciphers. Cryptography and Communications, 2017, 9, 523-543.	0.9	10
23	Cryptanalysis of an RSA variant with moduli N=p^rq^l . Journal of Mathematical Cryptology, 2017, 11, 117-130.	0.4	10
24	Partial Key Exposure: Generalized Framework to Attack RSA. Lecture Notes in Computer Science, 2011, , 76-92.	1.0	10
25	Revamped Differential-Linear Cryptanalysis onÂReduced Round ChaCha. Lecture Notes in Computer Science, 2022, , 86-114.	1.0	10
26	Cryptanalytic results on â€˜Dual CRTâ€™ and â€˜Common Primeâ€™ RSA. Designs, Codes, and Cryptography, 2013, 66, 157-174.	1.0	9
27	Proving the biases of Salsa and ChaCha in differential attack. Designs, Codes, and Cryptography, 2020, 88, 1827-1856.	1.0	9
28	Security Analysis of the RC4+ Stream Cipher. Lecture Notes in Computer Science, 2013, , 297-307.	1.0	8
29	A New Distinguisher on Grain v1 for 106 Rounds. Lecture Notes in Computer Science, 2015, , 334-344.	1.0	8
30	Partial Key Exposure Attack on CRT-RSA. Lecture Notes in Computer Science, 2009, , 473-484.	1.0	8
31	Some Combinatorial Results towards State Recovery Attack on RC4. Lecture Notes in Computer Science, 2011, , 204-214.	1.0	8
32	New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. Lecture Notes in Computer Science, 2013, , 222-239.	1.0	8
33	Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. Lecture Notes in Computer Science, 2015, , 350-369.	1.0	8
34	Model Selection Approach for Distributed Fault Detection in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 2014, 10, 148234.	1.3	8
35	Hypothesis testing and decision theoretic approach for fault detection in wireless sensor networks. International Journal of Parallel, Emergent and Distributed Systems, 2015, 30, 262-285.	0.7	7
36	A theoretical investigation on the distinguishers of Salsa and ChaCha. Discrete Applied Mathematics, 2021, 302, 147-162.	0.5	7

#	Article	IF	Citations
37	Revisiting Cryptanalysis on ChaCha From Crypto 2020 and Eurocrypt 2021. IEEE Transactions on Information Theory, 2022, 68, 6114-6133.	1.5	7
38	Cryptanalysis of Variants of RSA with Multiple Small Secret Exponents. Lecture Notes in Computer Science, 2015, , 105-123.	1.0	6
39	Factoring RSA Modulus Using Prime Reconstruction from Random Known Bits. Lecture Notes in Computer Science, 2010, , 82-99.	1.0	6
40	PARTIAL KEY EXPOSURE ATTACKS ON RSA AND ITS VARIANT BY GUESSING A FEW BITS OF ONE OF THE PRIME FACTORS. Bulletin of the Korean Mathematical Society, 2009, 46, 721-741.	0.3	6
41	Side Channel Attack to Actual Cryptanalysis: Breaking CRT-RSA with Low Weight Decryption Exponents. Lecture Notes in Computer Science, 2012, , 476-493.	1.0	5
42	Proving TLS-attack related open biases of RC4. Designs, Codes, and Cryptography, 2015, 77, 231-253.	1.0	5
43	Solving a class of modular polynomial equations and its relation to modular inversion hidden number problem and inversive congruential generator. Designs, Codes, and Cryptography, 2018, 86, 1997-2033.	1.0	5
44	Improved Partial Key Exposure Attacks on RSA by Guessing a Few Bits of One of the Prime Factors. Lecture Notes in Computer Science, 2009, , 37-51.	1.0	5
45	Some Results on Related Key-IV Pairs of Grain. Lecture Notes in Computer Science, 2012, , 94-110.	1.0	5
46	Proving empirical key-correlations in RC4. Information Processing Letters, 2014, 114, 234-238.	0.4	4
47	Some results on Fruit. Designs, Codes, and Cryptography, 2019, 87, 349-364.	1.0	4
48	New Results on Modular Inversion Hidden Number Problem and Inversive Congruential Generator. Lecture Notes in Computer Science, 2019, , 297-321.	1.0	4
49	Differential fault location identification by machine learning. CAAI Transactions on Intelligence Technology, 2021, 6, 17-24.	3.4	4
50	Results on significant anomalies of state values after key scheduling algorithm in RC4. IET Information Security, 2017, 11, 267-272.	1.1	3
51	Cryptanalysis of elliptic curve hidden number problem from PKC 2017. Designs, Codes, and Cryptography, 2020, 88, 341-361.	1.0	3
52	Efficient CRT-RSA Decryption for Small Encryption Exponents. Lecture Notes in Computer Science, 2010, , 26-40.	1.0	3
53	Some applications of lattice based root finding techniques. Advances in Mathematics of Communications, 2010, 4, 519-531.	0.4	3
54	Revisiting design principles of Salsa and ChaCha. Advances in Mathematics of Communications, 2019, 13, 689-704.	0.4	3

#	Article	IF	Citations
55	COUNTING HERON TRIANGLES WITH CONSTRAINTS. , 2014, , 24-40.		2
56	On acyclic edge-coloring of the complete bipartite graphs <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.gif" display="inline" overflow="scroll"><mml:msub><mml:mrow><mml:mi>K</mml:mi></mml:mrow><mml:mrow><mml:mn>2</mml:mn><mml:mi>p</mml for odd prime <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si2.gif" di. Discrete Mathematics, 2016, 339, 72-77.	0.4	2
57	Revisiting (nested) Roos bias in RC4 key scheduling algorithm. Designs, Codes, and Cryptography, 2017, 82, 131-148.	1.0	2
58	Settling the mystery of Zr = r in RC4. Cryptography and Communications, 2019, 11, 697-715.	0.9	2
59	Partial Key Exposure Attack on CRT-RSA. Lecture Notes in Computer Science, 2014, , 255-264.	1.0	2
60	Relaxing IND-CCA: Indistinguishability against Chosen Ciphertext Verification Attack. Lecture Notes in Computer Science, 2012, , 63-76.	1.0	2
61	A state bit recovery algorithm with TMDTO attack on Lizard and Grain-128a. Designs, Codes, and Cryptography, 2022, 90, 489.	1.0	2
62	On Universality of Quantum Fourier Transform. Chinese Physics Letters, 2012, 29, 030303.	1.3	1
63	On acyclic edge-coloring of complete bipartite graphs. Discrete Mathematics, 2017, 340, 481-493.	0.4	1
64	Some Conditional Cube Testers for Grain-128a of Reduced Rounds. IEEE Transactions on Computers, 2021, , 1-1.	2.4	1
65	Some Cryptanalytic Results on TRIAD. Lecture Notes in Computer Science, 2019, , 160-174.	1.0	1
66	A New Class of Weak Encryption Exponents in RSA. Lecture Notes in Computer Science, 2008, , 337-349.	1.0	1
67	Publishing Upper Half of RSA Decryption Exponent. Lecture Notes in Computer Science, 2010, , 25-39.	1.0	1
68	Error Correction of Partially Exposed RSA Private Keys from MSB Side. Lecture Notes in Computer Science, 2013, , 345-359.	1.0	1
69	Cryptanalysis of Multi-Prime $$varPhi $$ -Hiding Assumption. Lecture Notes in Computer Science, 2016, , 440-453.	1.0	1
70	On One-Dimensional Linear Minimal Codes Over Finite (Commutative) Rings. IEEE Transactions on Information Theory, 2022, 68, 2990-2998.	1.5	1
71	Revisiting orthogonal lattice attacks on approximate common divisor problems. Theoretical Computer Science, 2022, 911, 55-69.	0.5	1
72	Generalization of Roos bias in RC4 and some results on key-keystream relations. Journal of Mathematical Cryptology, 2018, 12, 43-56.	0.4	0

#	Article	IF	Citations
73	Analysis of Hidden Number Problem with Hidden Multiplier. Advances in Mathematics of Communications, 2017, 11, 805-811.	0.4	0
74	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
75	Some results on lightweight stream ciphers Fountain v1 & Lizard. Advances in Mathematics of Communications, 2020, .	0.4	0
76	Differential faultt attack on DEFAULT. Advances in Mathematics of Communications, 2022, .	0.4	0