Subhamoy Maitra

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/6390557/publications.pdf Version: 2024-02-01



#	Article	IF	CITATIONS
1	Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Designs, Codes, and Cryptography, 2006, 40, 41-58.	1.6	197
2	Nonlinearity Bounds and Constructions of Resilient Boolean Functions. Lecture Notes in Computer Science, 2000, , 515-532.	1.3	127
3	Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class. IEEE Transactions on Information Theory, 2007, 53, 1743-1751.	2.4	112
4	Rotation symmetric Boolean functions—Count and cryptographic properties. Discrete Applied Mathematics, 2008, 156, 1567-1580.	0.9	105
5	Construction of Nonlinear Boolean Functions with Important Cryptographic Properties. Lecture Notes in Computer Science, 2000, , 485-506.	1.3	94
6	Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Lecture Notes in Computer Science, 2004, , 92-106.	1.3	82
7	Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity. Lecture Notes in Computer Science, 2005, , 98-111.	1.3	80
8	Investigations on Bent and Negabent Functions via the Nega-Hadamard Transform. IEEE Transactions on Information Theory, 2012, 58, 4064-4072.	2.4	59
9	A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design. International Journal of Information Security, 2006, 5, 105-114.	3.4	58
10	A Differential Fault Attack on the Grain Family of Stream Ciphers. Lecture Notes in Computer Science, 2012, , 122-139.	1.3	49
11	(Non-)Random Sequences from (Non-)Random Permutations—Analysis of RC4 Stream Cipher. Journal of Cryptology, 2014, 27, 67-108.	2.8	48
12	Evolving Boolean Functions Satisfying Multiple Criteria. Lecture Notes in Computer Science, 2002, , 246-259.	1.3	48
13	Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. Lecture Notes in Computer Science, 2004, , 161-177.	1.3	45
14	Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes. Theory of Computing Systems, 2002, 35, 39-57.	1.1	43
15	Chosen IV cryptanalysis on reduced round ChaCha and Salsa. Discrete Applied Mathematics, 2016, 208, 88-97.	0.9	43
16	Permutation After RC4 Key Scheduling Reveals the Secret Key. , 2007, , 360-377.		42
17	Almost Boolean Functions: The Design of Boolean Functions by Spectral Inversion. Computational Intelligence, 2004, 20, 450-462.	3.2	35
18	Differential Fault Attack against Grain Family with Very Few Faults and Minimal Assumptions. IEEE Transactions on Computers, 2015, 64, 1647-1657.	3.4	32

#	Article	IF	CITATIONS
19	Redefining the transparency order. Designs, Codes, and Cryptography, 2017, 82, 95-115.	1.6	32
20	On non-negligible bias of the first output byte of RC4 towards the first three bytes of the secret key. Designs, Codes, and Cryptography, 2008, 49, 123-134.	1.6	31
21	Approximate Integer Common Divisor Problem Relates to Implicit Factorization. IEEE Transactions on Information Theory, 2011, 57, 4002-4013.	2.4	31
22	Balancedness and correlation immunity of symmetric Boolean functions. Discrete Mathematics, 2007, 307, 2351-2358.	0.7	27
23	Results on rotation symmetric bent functions. Discrete Mathematics, 2009, 309, 2398-2409.	0.7	27
24	Attack on Broadcast RC4 Revisited. Lecture Notes in Computer Science, 2011, , 199-217.	1.3	26
25	Cryptographically significant Boolean functions with five valued Walsh spectra. Theoretical Computer Science, 2002, 276, 133-146.	0.9	25
26	Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity. , 2007, , 271-280.		25
27	A constructive count of rotation symmetric functions. Information Processing Letters, 2003, 88, 299-304.	0.6	24
28	New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4. Lecture Notes in Computer Science, 2008, , 253-269.	1.3	24
29	Construction of \$n\$ -Variable (\$nequiv 2 mod 4\$) Balanced Boolean Functions With Maximum Absolute Value in Autocorrelation Spectra \$. IEEE Transactions on Information Theory, 2018, 64, 393-402.	2.4	23
30	A Differential Fault Attack on the Grain Family under Reasonable Assumptions. Lecture Notes in Computer Science, 2012, , 191-208.	1.3	23
31	A Differential Fault Attack on MICKEY 2.0. Lecture Notes in Computer Science, 2013, , 215-232.	1.3	23
32	Cryptanalysis of RSA with more than one decryption exponent. Information Processing Letters, 2010, 110, 336-340. McFarland type construction for resilient Boolean functions on n variables (n even)	0.6	20
33	with nonlinearity <mml:math <br="" altimg="si10.gif" overflow="scroll">xmlns:xocs="http://www.elsevier.com/xml/xocs/dtd" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://www.elsevier.com/xml/ja/dtd" xmlns:ja="http://www.elsevier.com/xml/ja/dtd" xmlns:mml="http://www.w3.org/1998/Math/MathML"</mml:math>	0.9	18
34	xmins:tb="http://www.elsevier.com/xmi/common/table/dtd" xmins:sb="htt: Discrete Applied Mathemati Cryptanalysis of RSA with two decryption exponents. Information Processing Letters, 2010, 110, 178-181.	0.6	18
35	Improved differential fault attack on MICKEY 2.0. Journal of Cryptographic Engineering, 2015, 5, 13-29.	1.8	18
36	A Differential Fault Attack on Plantlet. IEEE Transactions on Computers, 2017, 66, 1804-1808.	3.4	18

#	Article	IF	CITATIONS
37	Preparing Dicke States on a Quantum Computer. IEEE Transactions on Quantum E	ngin e e9ing, 2	20 20, 1, 1-1
38	ldempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros. Designs, Codes, and Cryptography, 2008, 49, 95-103.	1.6	17
39	A complete characterization of the evolution of RC4 pseudo random generation algorithm. Journal of Mathematical Cryptology, 2008, 2, .	0.7	15
40	Patterson–Wiedemann Type Functions on 21 Variables With Nonlinearity Greater Than Bent Concatenation Bound. IEEE Transactions on Information Theory, 2016, 62, 2277-2282.	2.4	15
41	Observing biases in the state: case studies with Trivium and Trivia-SC. Designs, Codes, and Cryptography, 2017, 82, 351-375.	1.6	15
42	Patterson–Wiedemann construction revisited. Discrete Mathematics, 2006, 306, 1540-1556.	0.7	14
43	Exact quantum algorithm to distinguish Boolean functions of different weights. Journal of Physics A: Mathematical and Theoretical, 2007, 40, 8441-8454.	2.1	13
44	Differential Fault Attack on Grain v1, ACORN v3 and Lizard. Lecture Notes in Computer Science, 2017, , 247-263.	1.3	13
45	Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile. Designs, Codes, and Cryptography, 2019, 87, 261-276.	1.6	13
46	Autocorrelation Properties of Correlation Immune Boolean Functions. Lecture Notes in Computer Science, 2001, , 242-253.	1.3	13
47	Hamming weights of correlation immune Boolean functions. Information Processing Letters, 1999, 71, 149-153.	0.6	12
48	Highly Nonlinear Balanced Boolean Functions with Very Good Autocorrelation Property. Electronic Notes in Discrete Mathematics, 2001, 6, 481-490.	0.4	12
49	Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics. Information Processing Letters, 2002, 83, 281-286.	0.6	12
50	Some observations on HC-128. Designs, Codes, and Cryptography, 2011, 59, 231-245.	1.6	12
51	THE DEUTSCH–JOZSA ALGORITHM REVISITED IN THE DOMAIN OF CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS. International Journal of Quantum Information, 2005, 03, 359-370.	1.1	10
52	Application of Grover's algorithm to check non-resiliency of a Boolean function. Cryptography and Communications, 2016, 8, 401-413.	1.4	10
53	Probabilistic signature based generalized framework for differential fault analysis of stream ciphers. Cryptography and Communications, 2017, 9, 523-543.	1.4	10
54	A TMDTO Attack Against Lizard. IEEE Transactions on Computers, 2018, 67, 733-739.	3.4	10

#	Article	IF	CITATIONS
55	Cryptanalytic results on â€~Dual CRT' and â€~Common Prime' RSA. Designs, Codes, and Cryptography, 20 66, 157-174.)13 1.6	9
56	Tools in Analyzing Linear Approximation for Boolean Functions Related to FLIP. Lecture Notes in Computer Science, 2018, , 282-303.	1.3	9
57	Modifying Maiorana–McFarland Type Bent Functions for Good Cryptographic Properties and Efficient Implementation. SIAM Journal on Discrete Mathematics, 2019, 33, 238-256.	0.8	9
58	Analysis on Boolean Function in a Restricted (Biased) Domain. IEEE Transactions on Information Theory, 2020, 66, 1219-1231.	2.4	8
59	A Hybrid Design of Key Pre-distribution Scheme for Wireless Sensor Networks. Lecture Notes in Computer Science, 2005, , 228-238.	1.3	8
60	On Non-randomness of the Permutation After RC4 Key Scheduling. , 2007, , 100-109.		8
61	New Results on Generalization of Roos-Type Biases and Related Keystreams of RC4. Lecture Notes in Computer Science, 2013, , 222-239.	1.3	8
62	Dependence in IV-Related Bytes of RC4 Key Enhances Vulnerabilities in WPA. Lecture Notes in Computer Science, 2015, , 350-369.	1.3	8
63	Balancedness and Correlation Immunity of Symmetric Boolean Functions. Electronic Notes in Discrete Mathematics, 2003, 15, 176-181.	0.4	7
64	On biases of permutation and keystream bytes of RC4 towards the secret key. Cryptography and Communications, 2009, 1, 225-268.	1.4	7
65	Clauser–Horne–Shimony–Holt versus three-party pseudo-telepathy: on the optimal number of samples in device-independent quantum private query. Quantum Information Processing, 2018, 17, 1.	2.2	7
66	Minimum Distance between Bent and 1-Resilient Boolean Functions. Lecture Notes in Computer Science, 2004, , 143-160.	1.3	7
67	Analysis of the "Wavelet Tree Quantization―watermarking strategy and a modified robust scheme. Multimedia Systems, 2006, 12, 151-163.	4.7	6
68	On non-existence of bent–negabent rotation symmetric Boolean functions. Discrete Applied Mathematics, 2018, 236, 1-6.	0.9	6
69	On the existence and non-existence of some classes of bent–negabent functions. Applicable Algebra in Engineering, Communications and Computing, 2022, 33, 237-260.	0.5	6
70	Further Constructions of Resilient Boolean Functions with Very High Nonlinearity. , 2002, , 265-280.		6
71	On Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling. Lecture Notes in Computer Science, 2009, , 137-148.	1.3	6
72	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

#	Article	IF	CITATIONS
73	On affine (non)equivalence of Boolean functions. Computing (Vienna/New York), 2009, 85, 37-55.	4.8	5
74	Efficient quantum algorithms to construct arbitrary Dicke states. Quantum Information Processing, 2014, 13, 2049-2069.	2.2	5
75	Proving TLS-attack related open biases of RC4. Designs, Codes, and Cryptography, 2015, 77, 231-253.	1.6	5
76	The connection between quadratic bent–negabent functions and the Kerdock code. Applicable Algebra in Engineering, Communications and Computing, 2019, 30, 387-401.	0.5	5
77	Differential Fault Attack on SIMON with Very Few Faults. Lecture Notes in Computer Science, 2018, , 107-119.	1.3	4
78	New Long-Term Glimpse of RC4 Stream Cipher. Lecture Notes in Computer Science, 2013, , 230-238.	1.3	4
79	Clique Size in Sensor Networks with Key Pre-Distribution Based on Transversal Design. International Journal of Distributed Sensor Networks, 2005, 1, 345-354.	2.2	3
80	Analysis and Improvement of Transformation-Based Reversible Logic Synthesis. , 2013, , .		3
81	Certain Observations on ACORN v3 and Grain v1—Implications Towards TMDTO Attacks. Journal of Hardware and Systems Security, 2019, 3, 64-77.	1.3	3
82	On approximate real mutually unbiased bases in square dimension. Cryptography and Communications, 2021, 13, 321-329.	1.4	3
83	Efficient Quantum Algorithms Related to Autocorrelation Spectrum. Lecture Notes in Computer Science, 2019, , 415-432.	1.3	3
84	Some applications of lattice based root finding techniques. Advances in Mathematics of Communications, 2010, 4, 519-531.	0.7	3
85	Improved and practical proposal for measurement device independent quantum dialogue. Quantum Information Processing, 2021, 20, 1.	2.2	3
86	Further cryptographic properties of the multiplicative inverse function. Discrete Applied Mathematics, 2022, 307, 191-211.	0.9	3
87	Cryptographic Properties and Structure of Boolean Functions with Full Algebraic Immunity. , 2006, , .		2
88	Laced Boolean functions and subset sum problems in finite fields. Discrete Applied Mathematics, 2011, 159, 1059-1069.	0.9	2
89	Certain Observations on ACORN v3 and the Implications to TMDTO Attacks. Lecture Notes in Computer Science, 2017, , 264-280.	1.3	2
90	A Super-Set of PattersonWiedemann Functions: Upper Bounds and Possible Nonlinearities. SIAM Journal on Discrete Mathematics, 2018, 32, 106-122.	0.8	2

#	Article	IF	CITATIONS
91	Differential Fault Attack on Kreyvium & amp; FLIP. IEEE Transactions on Computers, 2020, , 1-1.	3.4	2
92	Resolvable block designs in construction of approximate real MUBs that are sparse. Cryptography and Communications, 2022, 14, 527-549.	1.4	2
93	Vectorial Boolean Functions with Very Low Differential-Linear Uniformity Using Maiorana-McFarland Type Construction. Lecture Notes in Computer Science, 2019, , 341-360.	1.3	2
94	Quantum Algorithms Related to \$\$extit{HN}\$\$ -Transforms of Boolean Functions. Lecture Notes in Computer Science, 2017, , 314-327.	1.3	2
95	Cryptanalysis of a secret sharing scheme. Quantum Information and Computation, 2013, 13, 178-180.	0.3	2
96	Following Forrelation – quantum algorithms in exploring Boolean functions' spectra. Advances in Mathematics of Communications, 2024, 18, 1-25.	0.7	2
97	How Do theÂArbiter PUFs Sample theÂBoolean Function Class?. Lecture Notes in Computer Science, 2022, , 111-130.	1.3	2
98	A scheme for conditional access-based systems using index locations of DCT coefficients. Journal of Real-Time Image Processing, 2017, 13, 363-373.	3.5	1
99	Distinguisher and nonâ€randomness of Grainâ€v1 for 112, 114 and 116Âinitialisation rounds with multipleâ€bit difference in IVs. IET Information Security, 2019, 13, 603-613.	1.7	1
100	Parity decision tree in classical–quantum separations for certain classes of Boolean functions. Quantum Information Processing, 2021, 20, 1.	2.2	1
101	Glimpses are forever in RC4 amidst the spectre of biases. Discrete Applied Mathematics, 2021, 298, 84-102.	0.9	1
102	A Super-Set of Patterson-Wiedemann Functions – Upper Bounds and Possible Nonlinearities. Lecture Notes in Computer Science, 2016, , 227-242.	1.3	1
103	RC4: Non-randomness in the Index j and Some Results on Its Cycles. Lecture Notes in Computer Science, 2019, , 95-114.	1.3	1
104	Differential Fault Attack onÂEspresso. Lecture Notes in Computer Science, 2021, , 271-286.	1.3	1
105	Patterson-Wiedemann Construction Revisited. Electronic Notes in Discrete Mathematics, 2003, 15, 85-90.	0.4	0
106	Secure Communication in Distributed Sensor Networks (DSN). , 0, , 407-438.		0
107	Further clarification on Mantin's Digraph Repetition Bias in RC4. Designs, Codes, and Cryptography, 2021, 89, 127-141.	1.6	0
108	Grover's Algorithm and Walsh Spectrum. SpringerBriefs in Computer Science, 2021, , 59-87.	0.2	0

#	Article	IF	CITATIONS
109	Construction of balanced vectorial Boolean functions with almost optimal nonlinearity and very low differential-linear uniformity. Finite Fields and Their Applications, 2021, 76, 101903.	1.0	0
110	On Hardware Implementation of Tang-Maitra Boolean Functions. Lecture Notes in Computer Science, 2018, , 111-127.	1.3	0
111	More Climpses of the RC4 Internal State Array. Lecture Notes in Computer Science, 2020, , 294-311.	1.3	Ο
112	A Heuristic Framework toÂSearch forÂApproximate Mutually Unbiased Bases. Lecture Notes in Computer Science, 2022, , 208-223.	1.3	0