List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/8859421/publications.pdf Version: 2024-02-01



#	Article	IF	CITATIONS
1	Minimal linear codes from weakly regular bent functions. Cryptography and Communications, 2022, 14, 415-431.	1.4	7
2	Two New Families of Quadratic APN Functions. IEEE Transactions on Information Theory, 2022, 68, 4761-4769.	2.4	4
3	Infinite Families of 3-Designs and 2-Designs From Almost MDS Codes. IEEE Transactions on Information Theory, 2022, 68, 4344-4353.	2.4	8
4	The number of affine equivalent classes and extended affine equivalent classes of vectorial Boolean functions. Discrete Applied Mathematics, 2021, 289, 477-491.	0.9	0
5	New Constructions of Complete Permutations. IEEE Transactions on Information Theory, 2021, , 1-1.	2.4	2
6	A Complete Characterization of the APN Property of a Class of Quadrinomials. IEEE Transactions on Information Theory, 2021, 67, 7535-7549.	2.4	2
7	On equivalence between known polynomial APN functions and power APN functions. Finite Fields and Their Applications, 2021, 71, 101762.	1.0	3
8	More permutations and involutions for constructing bent functions. Cryptography and Communications, 2021, 13, 459-473.	1.4	0
9	Further study of planar functions in characteristic two. Journal of Algebra, 2021, 573, 712-740.	0.7	1
10	Further Study of 2-to-1 Mappings Over F _{2ⁿ} . IEEE Transactions on Information Theory, 2021, 67, 3486-3496.	2.4	9
11	Binary Linear Codes With Few Weights From Two-to-One Functions. IEEE Transactions on Information Theory, 2021, 67, 4263-4275.	2.4	10
12	Finding Compositional Inverses of Permutations From the AGW Criterion. IEEE Transactions on Information Theory, 2021, 67, 4975-4985.	2.4	10
13	Autocorrelations of Vectorial Boolean Functions. Lecture Notes in Computer Science, 2021, , 233-253.	1.3	4
14	Cryptographically strong permutations from the butterfly structure. Designs, Codes, and Cryptography, 2021, 89, 737-761.	1.6	16
15	New constructions of involutions over finite fields. Cryptography and Communications, 2020, 12, 165-185.	1.4	14
16	A new algorithm on the minimal rational fraction representation of feedback with carry shift registers. Designs, Codes, and Cryptography, 2020, 88, 533-552.	1.6	2
17	Vulnerable Public Keys in NTRU Cryptosystem. Chinese Annals of Mathematics Series B, 2020, 41, 657-664.	0.4	0
18	Minimal linear codes from Maiorana-McFarland functions. Finite Fields and Their Applications, 2020, 65, 101688.	1.0	15

#	Article	IF	CITATIONS
19	On a conjecture about a class of permutation quadrinomials. Finite Fields and Their Applications, 2020, 66, 101690.	1.0	18
20	A link between two classes of permutation polynomials. Finite Fields and Their Applications, 2020, 63, 101641.	1.0	2
21	A New Construction of (<i>m</i> + <i>k</i> , <i>m</i>)-Functions with Low Differential Uniformity. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A, 850-855.	0.3	0
22	On Two-to-One Mappings Over Finite Fields. IEEE Transactions on Information Theory, 2019, 65, 7884-7895.	2.4	22
23	New Results About the Boomerang Uniformity of Permutation Polynomials. IEEE Transactions on Information Theory, 2019, 65, 7542-7553.	2.4	47
24	Three Classes of Minimal Linear Codes Over the Finite Fields of Odd Characteristic. IEEE Transactions on Information Theory, 2019, 65, 7067-7078.	2.4	24
25	Further study of 2-to-1 mappings over F ₂ ⁿ . , 2019, , .		2
26	Constructing infinite families of low differential uniformity (n,Âm)-functions with \$\$m>n/2\$\$ m > n / 2. Designs, Codes, and Cryptography, 2019, 87, 1577-1599.	1.6	1
27	Compositional inverses of permutation polynomials of the form xrh(xs) over finite fields. Cryptography and Communications, 2019, 11, 279-298.	1.4	19
28	New constructions of permutation polynomials of the form \$\$x^rhleft(x^{q-1}ight) \$\$ x r h x q. Designs, Codes, and Cryptography, 2018, 86, 2379-2405.	1.6	22
29	Permutation polynomials of the form cx + Tr q l. Cryptography and Communications, 2018, 10, 531-554.	1.4	29
30	A better bound for implicit factorization problem with shared middle bits. Science China Information Sciences, 2018, 61, 1.	4.3	2
31	New permutation trinomials constructed from fractional polynomials. Acta Arithmetica, 2018, 183, 101-116.	0.4	16
32	Constructions of negabent functions over finite fields. Cryptography and Communications, 2017, 9, 165-180.	1.4	12
33	An equivalent condition on the switching construction of differentially 4-uniform permutations on from the inverse function. International Journal of Computer Mathematics, 2017, 94, 1252-1267.	1.8	3
34	New classes of permutation binomials and permutation trinomials over finite fields. Finite Fields and Their Applications, 2017, 43, 69-85.	1.0	73
35	More constructions of differentially 4-uniform permutations on \$\${mathbb {F}}_{2^{2k}}\$ F 2 2 k. Designs, Codes, and Cryptography, 2016, 78, 391.	1.6	21
36	Construction of odd-Variable Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 853-855.	0.3	9

#	Article	IF	CITATIONS
37	New Results on the Boolean Functions That Can Be Expressed as the Sum of Two Bent Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 1584-1590.	0.3	1
38	New constructions of q-variable 1-resilient rotation symmetric functions over \$mathbb{F}_p \$. Science China Information Sciences, 2016, 59, 1.	4.3	7
39	A new method to investigate the CCZ-equivalence between functions with low differential uniformity. Finite Fields and Their Applications, 2016, 42, 165-186.	1.0	1
40	A New Approach to Constructing Quadratic Pseudo-Planar Functions Over \$ {mathbb F}_{2^{n}}\$. IEEE Transactions on Information Theory, 2016, 62, 6644-6658.	2.4	5
41	New Insights on AES-Like SPN Ciphers. Lecture Notes in Computer Science, 2016, , 605-624.	1.3	27
42	Permutation Trinomials Over Finite Fields with Even Characteristic. SIAM Journal on Discrete Mathematics, 2015, 29, 79-92.	0.8	69
43	2-Adic complexity of binary sequences with interleaved structure. Finite Fields and Their Applications, 2015, 33, 14-28.	1.0	18
44	On the Walsh spectrum of a family of quadratic APN functions with five terms. Science China Information Sciences, 2014, 57, 1-7.	4.3	2
45	A New Method to Compute the 2-Adic Complexity of Binary Sequences. IEEE Transactions on Information Theory, 2014, 60, 2399-2406.	2.4	40
46	Some results on the differential functions over finite fields. Applicable Algebra in Engineering, Communications and Computing, 2014, 25, 189-195.	0.5	3
47	A recursive construction of highly nonlinear resilient vectorial functions. Information Sciences, 2014, 269, 388-396.	6.9	3
48	On the differential uniformities of functions over finite fields. Science China Mathematics, 2013, 56, 1477-1484.	1.7	2
49	New construction of perfect sequence set and low correlation zone sequence set. Science China Information Sciences, 2013, 56, 1-8.	4.3	1
50	Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity. Science China Information Sciences, 2013, 56, 1-9.	4.3	8
51	A negative answer to Bracken–Tan–Tan's problem on differentially 4-uniform permutations overF2n. Finite Fields and Their Applications, 2013, 24, 55-65.	1.0	3
52	Constructing Differentially 4-Uniform Permutations Over <formula formulatype="inline"><tex Notation="TeX">\${BBF}_{2^{2k}}\$ </tex </formula> via the Switching Method. IEEE Transactions on Information Theory, 2013, 59, 4675-4686.	2.4	81
53	New constructions of semi-bent functions in polynomial forms. Mathematical and Computer Modelling, 2013, 57, 1139-1147.	2.0	14
54	Linear complexity of binary sequences with interleaved structure. IET Communications, 2013, 7, 1688-1696.	2.2	11

#	Article	IF	CITATIONS
55	On the Fourier Spectra of New APN Functions. SIAM Journal on Discrete Mathematics, 2013, 27, 791-801.	0.8	3
56	Generalized Construction of Boolean Function with Maximum Algebraic Immunity Using Univariate Polynomial Representation. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 360-362.	0.3	2
5 7	On the Balanced Elementary Symmetric Boolean Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 663-665.	0.3	1
58	A New Construction of Low-Correlation Zone Sequence Sets. , 2012, , .		1
59	NEW CONSTRUCTIONS OF VECTORIAL BOOLEAN FUNCTIONS WITH GOOD CRYPTOGRAPHIC PROPERTIES. International Journal of Foundations of Computer Science, 2012, 23, 749-760.	1.1	2
60	Construction of highly nonlinear resilient S-boxes with given degree. Designs, Codes, and Cryptography, 2012, 64, 241-253.	1.6	6
61	A note on linearized polynomials and the dimension of their kernels. Finite Fields and Their Applications, 2012, 18, 56-62.	1.0	10
62	On the number of rotation symmetric functions over <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si4.gif" display="inline" overflow="scroll"><mml:mi>G</mml:mi><mml:mi>F</mml:mi><mml:mrow><mml:mo>(</mml:mo><ml:mi>p< Mathematical and Computer Modelling, 2012, 55, 142-150.</ml:mi></mml:mrow></mml:math 	/mmi:mi>	<m²nl:mo>)</m²nl:mo>
63	A Comment on Algebraic Immunity of the Sum of Two Boolean Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95.A, 1187-1188.	0.3	Ο
64	Balanced <mml:math <br="" altimg="si6.gif" xmlns:mml="http://www.w3.org/1998/Math/MathML">display="inline" overflow="scroll"><mml:mn>2</mml:mn><mml:mi>p</mml:mi></mml:math> -variable rotation symmetric Boolean functions with maximum algebraic immunity. Applied Mathematics Letters, 2011, 24, 2093-2096.	2.7	15
65	Construction of Odd-Variable Resilient Boolean Functions with Optimal Degree. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 265-267.	0.3	5
66	On the number of rotation symmetric Boolean functions. Science China Information Sciences, 2010, 53, 537-545.	4.3	11
67	SQUARE attack on block ciphers with low algebraic degree. Science China Information Sciences, 2010, 53, 1988-1995.	4.3	6
68	Enumeration of balanced symmetric functions over. Information Processing Letters, 2010, 110, 544-548.	0.6	2
69	Multi-objective memetic evolution of ART-based classifiers. , 2010, , .		2
70	On the Covering Structures of Two Classes of Linear Codes From Perfect Nonlinear Functions. IEEE Transactions on Information Theory, 2009, 55, 70-82.	2.4	13
71	Constructing Symmetric Boolean Functions With Maximum Algebraic Immunity. IEEE Transactions on Information Theory, 2009, 55, 2406-2412.	2.4	71
72	New Cryptanalysis of Block Ciphers with Low Algebraic Degree. Lecture Notes in Computer Science, 2009, , 180-192.	1.3	9

#	Article	IF	CITATIONS
73	Impossible Differential Cryptanalysis of SNAKE-2. , 2009, , .		0
74	Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity. Lecture Notes in Computer Science, 2009, , 402-412.	1.3	15
75	Construction of Odd-Variable Boolean Function with Maximum Algebraic Immunity. Lecture Notes in Computer Science, 2009, , 109-117.	1.3	0
76	A New Construction of Boolean Functions with Maximum Algebraic Immunity. Lecture Notes in Computer Science, 2009, , 177-185.	1.3	3
77	Minimum Distance between Bent and Resilient Boolean Functions. Lecture Notes in Computer Science, 2009, , 219-232.	1.3	1
78	On the 2m-variable symmetric Boolean functions with maximum algebraic immunity. Science in China Series F: Information Sciences, 2008, 51, 120-127.	1.1	25
79	On the Construction of Boolean Functions With Optimal Algebraic Immunity. IEEE Transactions on Information Theory, 2008, 54, 1330-1334.	2.4	72
80	A Note on Symmetric Boolean Functions With Maximum Algebraic Immunity in Odd Number of Variables. IEEE Transactions on Information Theory, 2007, 53, 2908-2910.	2.4	44
81	Weight Support Technique and the Symmetric Boolean Functions with Maximum Algebraic Immunity on Even Number of Variables. Lecture Notes in Computer Science, 2007, , 271-282.	1.3	2
82	Differential and boomerang spectrums of some power permutations. Cryptography and Communications, 0, , 1.	1.4	7
83	On two conjectures about the intersection distribution. Journal of Algebraic Combinatorics, 0, , 1.	0.8	Ο