Sihem Mesnager

List of Publications by Year
in descending order

143	2,398	257357	289141
papers	citations	24 h-index	40 g-index

152	152	152	450
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	On those multiplicative subgroups of $${mathbb F}_{2^n}^*$$ which are Sidon sets and/or sum-free sets. Journal of Algebraic Combinatorics, 2022, 55, 43-59.	0.4	3
2	A new family of polyphase sequences with low correlation. Cryptography and Communications, 2022, 14, 135-144.	0.9	3
3	Constructions of Z-optimal Type-II quadriphase Z-complementary pairs. Discrete Mathematics, 2022, 345, 112685.	0.4	2
4	Survey on recent trends towards generalized differential and boomerang uniformities. Cryptography and Communications, 2022, 14, 691-735.	0.9	11
5	On One-Dimensional Linear Minimal Codes Over Finite (Commutative) Rings. IEEE Transactions on Information Theory, 2022, 68, 2990-2998.	1.5	1
6	Classification of the Codewords of Weights 16 and 18 of the Reed-Muller Code <i>RM(n-3,n)</i>. IEEE Transactions on Information Theory, 2022, 68, 940-952.	1.5	4
7	On Infinite Families of Narrow-Sense Antiprimitive BCH Codes Admitting 3-Transitive Automorphism Groups and Their Consequences. IEEE Transactions on Information Theory, 2022, 68, 3096-3107.	1.5	7
8	Generic Constructions of (Boolean and Vectorial) Bent Functions and Their Consequences. IEEE Transactions on Information Theory, 2022, 68, 2735-2751.	1.5	7
9	Linear codes from support designs of ternary cyclic codes. Designs, Codes, and Cryptography, 2022, 90, 681.	1.0	0
10	Constructions of Optimal Uniform Wide-Gap Frequency-Hopping Sequences. IEEE Transactions on Information Theory, 2022, 68, 692-700.	1.5	11
11	An STP-based model toward designing S-boxes with good cryptographic properties. Designs, Codes, and Cryptography, 2022, 90, 1179-1202.	1.0	3
12	A function field approach toward good polynomials for further results on optimal LRC codes. Finite Fields and Their Applications, 2022, 81, 102028.	0.6	1
13	On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. Designs, Codes, and Cryptography, 2022, 90, 1437-1461.	1.0	9
14	Solving <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.svg"><mml:msup><mml:mrow><mml:mi>X</mml:mi></mml:mrow><mml:mrow><mml:msup><mml:mrow><mml:mn>2</m linebreak="badbreak" linebreakstyle="after">+</mml:mo><mml:msup><mml:mrow><mml:mn>2</mml:mn></mml:mrow><mml:mrow><mml:mn>2</mml:mn linebreak="badbreak" linebreakstyle="after">+</mml:mo><mml:msup><mm. Finite Fields and Their Applications, 2022, 83, 102086.	0.6	1
15	Optimizing Inner Product Masking Scheme by a Coding Theory Approach. IEEE Transactions on Information Forensics and Security, 2021, 16, 220-235.	4.5	18
16	A construction method of balanced rotation symmetric Boolean functions on arbitrary even number of variables with optimal algebraic immunity. Designs, Codes, and Cryptography, 2021, 89, 1-17.	1.0	6
17	Linear codes with one-dimensional hull associated with Gaussian sums. Cryptography and Communications, 2021, 13, 225-243.	0.9	12
18	A direct proof of APN-ness of the Kasami functions. Designs, Codes, and Cryptography, 2021, 89, 441-446.	1.0	5

#	Article	IF	Citations
19	On correlation immune Boolean functions with minimum Hamming weight power of 2. IEEE Transactions on Information Theory, 2021, , 1-1.	1.5	0
20	Solving X+1â€¯+â€¯Xâ€¯+â€¯aâ€¯=â€¯0 over finite fields. Finite Fields and Their Applications, 2021, 70, 101797.	0.6	15
21	More permutations and involutions for constructing bent functions. Cryptography and Communications, 2021, 13, 459-473.	0.9	0
22	On constructions of weightwise perfectly balanced Boolean functions. Cryptography and Communications, 2021, 13, 951-979.	0.9	13
23	Investigation for 8-bit SKINNY-like S-boxes, analysis and applications. Cryptography and Communications, 2021, 13, 617.	0.9	0
24	Good polynomials for optimal LRC of low locality. Designs, Codes, and Cryptography, 2021, 89, 1639-1660.	1.0	3
25	Cyclic Bent Functions and Their Applications in Sequences. IEEE Transactions on Information Theory, 2021, 67, 3473-3485.	1.5	2
26	Further Study of 2-to-1 Mappings Over F_{2ⁿ}. IEEE Transactions on Information Theory, 2021, 67, 3486-3496.	1.5	9
27	Fast Algebraic Immunity of Boolean Functions and LCD Codes. IEEE Transactions on Information Theory, 2021, 67, 4828-4837.	1.5	3
28	Secondary constructions of (non)weakly regular plateaued functions over finite fields. Turkish Journal of Mathematics, 2021, 45, 2295-2306.	0.3	6
29	Post-Quantum Secure Inner Product Functional Encryption Using Multivariate Public Key Cryptography. Mediterranean Journal of Mathematics, 2021, 18, 1.	0.4	4
30	A Novel Application of Boolean Functions With High Algebraic Immunity in Minimal Codes. IEEE Transactions on Information Theory, 2021, 67, 6856-6867.	1.5	3
31	Investigations on c-(Almost) Perfect Nonlinear Functions. IEEE Transactions on Information Theory, 2021, 67, 6916-6925.	1.5	25
32	On Hulls of Some Primitive BCH Codes and Self-Orthogonal Codes. IEEE Transactions on Information Theory, 2021, 67, 6442-6455.	1.5	12
33	Complete solution over <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.svg"><mml:msub><mml:mrow><mml:mi mathvariant="double-struck">F</mml:mi></mml:mrow><mml:mrow><mml:msup><mml:mrow><mml:mi>p</mml:mi></mml:mrow><mml:mrow><m of the equation <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si2.svg"><mml:msup><mml:mrow><mml:mi>X</mml:mi></mml:mrow><mml:mrow><mml:msup><mml:mrow><mml:mi>p</mml:mi> Finite Fields and Their Applications, 2021, 76, 101902.	0.6	5
34	Secret sharing schemes based on the dual of Golay codes. Cryptography and Communications, 2021, 13, 1025-1041.	0.9	1
35	On the Menezes-Teske-Weng conjecture. Cryptography and Communications, 2020, 12, 19-27.	0.9	4
36	A proof of the Beierleâ€“Kranzâ€“Leander conjecture related to lightweight multiplication in $$mathbb {F}_{2^n}$$. Designs, Codes, and Cryptography, 2020, 88, 51-62.	1.0	1

#	Article	IF	Citations
37	On generalized hyper-bent functions. Cryptography and Communications, 2020, 12, 455-468.	0.9	0
38	A class of narrow-sense BCH codes over $$mathbb {F}_q$$ of length $$rac{q^m-1}{2}$$. Designs, Codes, and Cryptography, 2020, 88, 413-427.	1.0	7
39	On the number of the rational zeros of linearized polynomials and the second-order nonlinearity of cubic Boolean functions. Cryptography and Communications, 2020, 12, 659-674.	0.9	5
40	Codebooks from generalized bent <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e146" altimg="si4.svg"><mml:msub><mml:mrow><mml:mi mathvariant="double-struck">Z</mml:mi></mml:mrow><mml:mrow><mml:mn>4</mml:mn></mml:mrow></mml:msub></mml:math>-v quadratic forms. Discrete Mathematics, 2020, 343, 111736.	0.4	3
41	Several Classes of Minimal Linear Codes With Few Weights From Weakly Regular Plateaued Functions. IEEE Transactions on Information Theory, 2020, 66, 2296-2310.	1.5	45
42	New characterizations and construction methods of bent and hyper-bent Boolean functions. Discrete Mathematics, 2020, 343, 112081.	0.4	3
43	Solving some affine equations over finite fields. Finite Fields and Their Applications, 2020, 68, 101746.	0.6	2
44	Threshold-Based Post-Quantum Secure Verifiable Multi-Secret Sharing for Distributed Storage Blockchain. Mathematics, 2020, 8, 2218.	1.1	13
45	Recent results and problems on constructions of linear codes from cryptographic functions. Cryptography and Communications, 2020, 12, 965-986.	0.9	26
46	On the boomerang uniformity of quadratic permutations. Designs, Codes, and Cryptography, 2020, 88, 2233-2246.	1.0	25
47	Minimal Linear Codes From Characteristic Functions. IEEE Transactions on Information Theory, 2020, 66, 5404-5413.	1.5	25
48	Constructions of optimal locally recoverable codes via Dickson polynomials. Designs, Codes, and Cryptography, 2020, 88, 1759-1780.	1.0	7
49	Solving $x+x^{2^{l}}+cdots +x^{2^{ml}}=a$ over $mathbb {F}_{2^{n}}$. Cryptography and Communications, 2020, 12, 809-817.	0.9	8
50	Solving <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.svg"><mml:msup><mml:mrow><mml:mi>x</mml:mi></mml:mrow><mml:mrow><mml:msup><mml:mrow><mml:mn>2</mml:m linebreak="badbreak" linebreakstyle="after">+</mml:mo><mml:mn>1</mml:mn></mml:mrow></mml:msup><mml:mo linebreak="goodbreak" linebreakstyle="after">+</mml:mo><mml:mi>x</mml:mi><mml:mo linebreak="goodbreak" linebreakstyle="after">+</mml:mo><mml:mi>a</mml:mi><mml:mo. Finite Fields a	0.6	15
51	Constructions of Self-Orthogonal Codes From Hulls of BCH Codes and Their Parameters. IEEE Transactions on Information Theory, 2020, 66, 6774-6785.	1.5	24
52	New characterizations for the multi-output correlation-immune Boolean functions. Discrete Mathematics, 2020, 343, 112082.	0.4	1
53	New Characterization and Parametrization of LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 39-49.	1.5	40
54	On Two-to-One Mappings Over Finite Fields. IEEE Transactions on Information Theory, 2019, 65, 7884-7895.	1.5	22

#	Article	IF	Citations
55	Linear codes with small hulls in semi-primitive case. Designs, Codes, and Cryptography, 2019, 87, 3063-3075.	1.0	17
56	Multiple characters transforms and generalized Boolean functions. Cryptography and Communications, 2019, 11, 1247-1260.	0.9	4
57	Some (almost) optimally extendable linear codes. Designs, Codes, and Cryptography, 2019, 87, 2813-2834.	1.0	3
58	Several new classes of self-dual bent functions derived from involutions. Cryptography and Communications, 2019, 11, 1261-1273.	0.9	9
59	Further study on the maximum number of bent components of vectorial functions. Designs, Codes, and Cryptography, 2019, 87, 2597-2610.	1.0	9
60	On Plateaued Functions, Linear Structures and Permutation Polynomials. Lecture Notes in Computer Science, 2019, , 217-235.	1.0	0
61	On Good Polynomials over Finite Fields for Optimal Locally Recoverable Codes. Lecture Notes in Computer Science, 2019, , 257-268.	1.0	0
62	Strongly Regular Graphs from Weakly Regular Plateaued Functions*. , 2019, , .		1
63	Further study of 2-to-1 mappings over F₂ ⁿ. , 2019, , .		2
64	Weightwise perfectly balanced functions with high weightwise nonlinearity profile. Designs, Codes, and Cryptography, 2019, 87, 1797-1813.	1.0	16
65	Linear codes from weakly regular plateaued functions and their secret sharing schemes. Designs, Codes, and Cryptography, 2019, 87, 463-480.	1.0	46
66	On $sigma$ -LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 1694-1704.	1.5	29
67	On the nonlinearity of Boolean functions with restricted input. Cryptography and Communications, 2019, 11, 63-76.	0.9	24
68	On <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" id="mml1" display="inline" overflow="scroll" altimg="si1.gif"><mml:mi>q</mml:mi></mml:math>-ary plateaued functions over <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" id="mml2" display="inline" overflow="scroll" altimg="si2.gif"><mml:msub><mml:mrow><mml:mi mathvariant="double-struck">F</mml:mi></mml:mrow><mml:mrow><mml:mi>q</mml:mi></mml:mrow></mml:msub></mml:math> and their explicit characterizations. European Journal of Combinatorics, 2019, 80, 71-81.	0.5	8
69	Statistical integral distinguisher with multi-structure and its application on AES-like ciphers. Cryptography and Communications, 2018, 10, 755-776.	0.9	2
70	Euclidean and Hermitian LCD MDS codes. Designs, Codes, and Cryptography, 2018, 86, 2605-2618.	1.0	75
71	Linear Codes Over $mathbb F_q$ Are Equivalent to LCD Codes for $q>3$. IEEE Transactions on Information Theory, 2018, 64, 3010-3017.	1.5	114
72	Complementary Dual Algebraic Geometry Codes. IEEE Transactions on Information Theory, 2018, 64, 2390-2397.	1.5	45

#	Article	IF	Citations
73	Bent Functions From Involutions Over ${mathbb F}_{2^{n}}$. IEEE Transactions on Information Theory, 2018, 64, 2979-2986.	1.5	16
74	Classification of Bent Monomials, Constructions of Bent Multinomials and Upper Bounds on the Nonlinearity of Vectorial Functions. IEEE Transactions on Information Theory, 2018, 64, 367-383.	1.5	14
75	2-Correcting Lee Codes: (Quasi)-Perfect Spectral Conditions and Some Constructions. IEEE Transactions on Information Theory, 2018, 64, 3031-3041.	1.5	4
76	New Constructions of Optimal Locally Recoverable Codes via Good Polynomials. IEEE Transactions on Information Theory, 2018, 64, 889-899.	1.5	31
77	On the p-ary (cubic) bent and plateaued (vectorial) functions. Designs, Codes, and Cryptography, 2018, 86, 1865-1892.	1.0	6
78	Further Results on Generalized Bent Functions and Their Complete Characterization. IEEE Transactions on Information Theory, 2018, 64, 5441-5452.	1.5	18
79	Characterizations of Partially Bent and Plateaued Functions over Finite Fields. Lecture Notes in Computer Science, 2018, , 224-241.	1.0	3
80	A comparison of Carlet's second-order nonlinearity bounds. International Journal of Computer Mathematics, 2017, 94, 427-436.	1.0	1
81	On the nonlinearity of S-boxes and linear codes. Cryptography and Communications, 2017, 9, 345-361.	0.9	8
82	Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptography and Communications, 2017, 9, 71-84.	0.9	67
83	Bent functions linear on elements of some classical spreads and presemifields spreads. Cryptography and Communications, 2017, 9, 3-21.	0.9	6
84	New Bent Functions from Permutations and Linear Translators. Lecture Notes in Computer Science, 2017, , 282-297.	1.0	7
85	Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions. Lecture Notes in Computer Science, 2017, , 328-345.	1.0	5
86	Generalized Plateaued Functions and Admissible (Plateaued) Functions. IEEE Transactions on Information Theory, 2017, 63, 6139-6148.	1.5	13
87	Decomposing Generalized Bent and Hyperbent Functions. IEEE Transactions on Information Theory, 2017, 63, 7804-7812.	1.5	17
88	Explicit constructions of bent functions from pseudo-planar functions. Advances in Mathematics of Communications, 2017, 11, 293-299.	0.4	2
89	On constructions of bent, semi-bent and five valued spectrum functions from old bent functions. Advances in Mathematics of Communications, 2017, 11, 339-345.	0.4	15
90	On construction of bent functions involving symmetric functions and their duals. Advances in Mathematics of Communications, 2017, 11, 347-352.	0.4	5

#	Article	IF	Citations
91	Fast algebraic immunity of Boolean functions. Advances in Mathematics of Communications, 2017, 11, 373-377.	0.4	2
92	Boolean Functions and Cryptography. , 2016, , 45-68.		1
93	Bent Functions. , 2016, , .		161
94	Linear Codes from Bent, Semi-bent and Almost Bent Functions. , 2016, , 529-540.		0
95	Plateaued Functions: Generalities and Characterizations. , 2016, , 417-464.		0
96	On constructions of bent functions from involutions. , 2016, , .		23
97	Four decades of research on bent functions. Designs, Codes, and Cryptography, 2016, 78, 5-50.	1.0	156
98	Results on Characterizations of Plateaued Functions in Arbitrary Characteristic. Lecture Notes in Computer Science, 2016, , 17-30.	1.0	10
99	Involutions Over the Galois Field. IEEE Transactions on Information Theory, 2016, 62, 2266-2276.	1.5	43
100	Further constructions of infinite families of bent functions from new permutations and their duals. Cryptography and Communications, 2016, 8, 229-246.	0.9	23
101	Yet another variation on minimal linear codes. Advances in Mathematics of Communications, 2016, 10, 53-61.	0.4	5
102	Bent Functions: Primary Constructions (Part I). , 2016, , 93-104.		0
103	Bent Vectorial Functions. , 2016, , 305-327.		1
104	Generalities on Boolean Functions and p-Ary Functions. , 2016, , 1-15.		3
105	Class $$mathcal{H}$$, Niho Bent Functions and o-Polynomials. , 2016, , 153-170.		0
106	Bent Functions and (Partial-)spreads. , 2016, , 345-385.		0
107	Bent Functions in Arbitrary Characteristic. , 2016, , 329-344.		0
108	Bent Functions-Generalities. , 2016, , 69-91.		2

#	Article	IF	Citations
109	Bent vectorial functions and linear codes from o-polynomials. Designs, Codes, and Cryptography, 2015, 77, 99-116.	1.0	21
110	Cyclic codes and algebraic immunity of Boolean functions. , 2015, , .		3
111	Optimal Codebooks From Binary Codes Meeting the Levenshtein Bound. IEEE Transactions on Information Theory, 2015, 61, 6526-6535.	1.5	30
112	On Existence (Based on an Arithmetical Problem) and Constructions of Bent Functions. Lecture Notes in Computer Science, 2015, , 3-19.	1.0	9
113	Bent and Semi-bent Functions via Linear Translators. Lecture Notes in Computer Science, 2015, , 205-224.	1.0	9
114	Sphere coverings and identifying codes. Designs, Codes, and Cryptography, 2014, 70, 3-7.	1.0	2
115	Several New Infinite Families of Bent Functions and Their Duals. IEEE Transactions on Information Theory, 2014, 60, 4397-4407.	1.5	97
116	Characterizations of Plateaued and Bent Functions in Characteristic $$p$$. Lecture Notes in Computer Science, 2014, , 72-82.	1.0	17
117	On Minimal and Quasi-minimal Linear Codes. Lecture Notes in Computer Science, 2013, , 85-98.	1.0	36
118	Hyperbent Functions via Dillon-Like Exponents. IEEE Transactions on Information Theory, 2013, 59, 3215-3232.	1.5	31
119	An efficient characterization of a family of hyper-bent functions with multiple trace terms. Journal of Mathematical Cryptology, 2013, 7, .	0.4	6
120	Semi-bent Functions from Oval Polynomials. Lecture Notes in Computer Science, 2013, , 1-15.	1.0	13
121	Further Results on Niho Bent Functions. IEEE Transactions on Information Theory, 2012, 58, 6979-6985.	1.5	38
122	Dickson Polynomials, Hyperelliptic Curves and Hyper-bent Functions. Lecture Notes in Computer Science, 2012, , 40-52.	1.0	8
123	Semi-bent Functions with Multiple Trace Terms and Hyperelliptic Curves. Lecture Notes in Computer Science, 2012, , 18-36.	1.0	8
124	Hyper-bent functions via Dillon-like exponents. , 2012, , .		4
125	On Semibent Boolean Functions. IEEE Transactions on Information Theory, 2012, 58, 3287-3292.	1.5	36
126	Generalized Witness Sets. , 2011, , .		0

#	Article	IF	Citations
127	Bent and Hyper-Bent Functions in Polynomial Form and Their Link With Some Exponential Sums and Dickson Polynomials. IEEE Transactions on Information Theory, 2011, 57, 5996-6009.	1.5	59
128	Semibent Functions From Dillon and Niho Exponents, Kloosterman Sums, and Dickson Polynomials. IEEE Transactions on Information Theory, 2011, 57, 7443-7458.	1.5	39
129	A new class of bent and hyper-bent Boolean functions in polynomial forms. Designs, Codes, and Cryptography, 2011, 59, 265-279.	1.0	42
130	On DillonÊ¼s class H of bent functions, Niho bent functions and o-polynomials. Journal of Combinatorial Theory - Series A, 2011, 118, 2392-2410.	0.5	82
131	On the dual of bent functions with 2^r Niho exponents. , 2011, , .		9
132	On the Link of Some Semi-bent Functions with Kloosterman Sums. Lecture Notes in Computer Science, 2011, , 263-272.	1.0	6
133	Binary Kloosterman Sums with Value 4. Lecture Notes in Computer Science, 2011, , 61-78.	1.0	4
134	On the construction of bent vectorial functions. International Journal of Information and Coding Theory, 2010, 1, 133.	0.3	16
135	Recent results on bent and hyper-bent functions and their link with some exponential sums. , 2010, , .		4
136	A New Family of Hyper-Bent Boolean Functions in Polynomial Form. Lecture Notes in Computer Science, 2009, , 402-417.	1.0	27
137	Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity. IEEE Transactions on Information Theory, 2008, 54, 3656-3662.	1.5	28
138	Secret-sharing schemes based on self-dual codes. , 2008, , .		28
139	Improving the Upper Bounds on the Covering Radii of Binary Reedâ€“Muller Codes. IEEE Transactions on Information Theory, 2007, 53, 162-173.	1.5	51
140	Preimages of p â^'Linearized Polynomials over ${mathbb {F}}_{p}$. Cryptography and Communications, 0, , 1.	0.9	0
141	Cryptanalysis of the AEAD and hash algorithm DryGASCON. Cryptography and Communications, 0, , 1.	0.9	1
142	Constructions of two-dimensional Z-complementary array pairs with large ZCZ ratio. Designs, Codes, and Cryptography, 0, , 1.	1.0	2
143	Explicit values of the DDT, the BCT, the FBCT, and the FBDT of the inverse, the gold, and the Bracken-Leander S-boxes. Cryptography and Communications, 0, , .	0.9	4