

# Sihem Mesnager

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/9100061/publications.pdf>

Version: 2024-02-01

143  
papers

2,398  
citations

257357

24  
h-index

289141

40  
g-index

152  
all docs

152  
docs citations

152  
times ranked

450  
citing authors

#	ARTICLE	IF	CITATIONS
1	Bent Functions. , 2016, , .		161
2	Four decades of research on bent functions. Designs, Codes, and Cryptography, 2016, 78, 5-50.	1.0	156
3	Linear Codes Over $\mathbb{F}_q$ Are Equivalent to LCD Codes for $q \geq 3$ . IEEE Transactions on Information Theory, 2018, 64, 3010-3017.	1.5	114
4	Several New Infinite Families of Bent Functions and Their Duals. IEEE Transactions on Information Theory, 2014, 60, 4397-4407.	1.5	97
5	On Dillon's class H of bent functions, Niho bent functions and o-polynomials. Journal of Combinatorial Theory - Series A, 2011, 118, 2392-2410.	0.5	82
6	Euclidean and Hermitian LCD MDS codes. Designs, Codes, and Cryptography, 2018, 86, 2605-2618.	1.0	75
7	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
8	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
9	Improving the Upper Bounds on the Covering Radii of Binary Reed-Muller Codes. IEEE Transactions on Information Theory, 2007, 53, 162-173.	1.5	51
10	Linear codes from weakly regular plateaued functions and their secret sharing schemes. Designs, Codes, and Cryptography, 2019, 87, 463-480.	1.0	46
11	Complementary Dual Algebraic Geometry Codes. IEEE Transactions on Information Theory, 2018, 64, 2390-2397.	1.5	45
12	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
13	Involutions Over the Galois Field. IEEE Transactions on Information Theory, 2016, 62, 2266-2276.	1.5	43
14	A new class of bent and hyper-bent Boolean functions in polynomial forms. Designs, Codes, and Cryptography, 2011, 59, 265-279.	1.0	42
15	New Characterization and Parametrization of LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 39-49.	1.5	40
16	Semibent Functions From Dillon and Niho Exponents, Kloosterman Sums, and Dickson Polynomials. IEEE Transactions on Information Theory, 2011, 57, 7443-7458.	1.5	39
17	Further Results on Niho Bent Functions. IEEE Transactions on Information Theory, 2012, 58, 6979-6985.	1.5	38
18	On Semibent Boolean Functions. IEEE Transactions on Information Theory, 2012, 58, 3287-3292.	1.5	36

#	ARTICLE	IF	CITATIONS
19	On Minimal and Quasi-minimal Linear Codes. Lecture Notes in Computer Science, 2013, , 85-98.	1.0	36
20	Hyperbent Functions via Dillon-Like Exponents. IEEE Transactions on Information Theory, 2013, 59, 3215-3232.	1.5	31
21	New Constructions of Optimal Locally Recoverable Codes via Good Polynomials. IEEE Transactions on Information Theory, 2018, 64, 889-899.	1.5	31
22	Optimal Codebooks From Binary Codes Meeting the Levenshtein Bound. IEEE Transactions on Information Theory, 2015, 61, 6526-6535.	1.5	30
23	On $\sigma$ -LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 1694-1704.	1.5	29
24	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
25	Secret-sharing schemes based on self-dual codes. , 2008, , .		28
26	A New Family of Hyper-Bent Boolean Functions in Polynomial Form. Lecture Notes in Computer Science, 2009, , 402-417.	1.0	27
27	Recent results and problems on constructions of linear codes from cryptographic functions. Cryptography and Communications, 2020, 12, 965-986.	0.9	26
28	On the boomerang uniformity of quadratic permutations. Designs, Codes, and Cryptography, 2020, 88, 2233-2246.	1.0	25
29	Minimal Linear Codes From Characteristic Functions. IEEE Transactions on Information Theory, 2020, 66, 5404-5413.	1.5	25
30	Investigations on $\mathcal{C}$ -(Almost) Perfect Nonlinear Functions. IEEE Transactions on Information Theory, 2021, 67, 6916-6925.	1.5	25
31	On the nonlinearity of Boolean functions with restricted input. Cryptography and Communications, 2019, 11, 63-76.	0.9	24
32	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
33	On constructions of bent functions from involutions. , 2016, , .		23
34	Further constructions of infinite families of bent functions from new permutations and their duals. Cryptography and Communications, 2016, 8, 229-246.	0.9	23
35	On Two-to-One Mappings Over Finite Fields. IEEE Transactions on Information Theory, 2019, 65, 7884-7895.	1.5	22
36	Bent vectorial functions and linear codes from o-polynomials. Designs, Codes, and Cryptography, 2015, 77, 99-116.	1.0	21

#	ARTICLE	IF	CITATIONS
37	Further Results on Generalized Bent Functions and Their Complete Characterization. IEEE Transactions on Information Theory, 2018, 64, 5441-5452.	1.5	18
38	Optimizing Inner Product Masking Scheme by a Coding Theory Approach. IEEE Transactions on Information Forensics and Security, 2021, 16, 220-235.	4.5	18
39	Decomposing Generalized Bent and Hyperbent Functions. IEEE Transactions on Information Theory, 2017, 63, 7804-7812.	1.5	17
40	Linear codes with small hulls in semi-primitive case. Designs, Codes, and Cryptography, 2019, 87, 3063-3075.	1.0	17
41	Characterizations of Plateaued and Bent Functions in Characteristic $2^p$ . Lecture Notes in Computer Science, 2014, , 72-82.	1.0	17
42	On the construction of bent vectorial functions. International Journal of Information and Coding Theory, 2010, 1, 133.	0.3	16
43	Bent Functions From Involutions Over $\mathbb{F}_{2^n}$ . IEEE Transactions on Information Theory, 2018, 64, 2979-2986.	1.5	16
44	Weightwise perfectly balanced functions with high weightwise nonlinearity profile. Designs, Codes, and Cryptography, 2019, 87, 1797-1813.	1.0	16
45	<a href="https://www.w3.org/1998/Math/MathML">https://www.w3.org/1998/Math/MathML</a> $\sum_{x \in \mathbb{F}_2^n} (-1)^{x \cdot a} \chi(x)$	0.6	15
46	Solving $X^2 + aX + b = 0$ over finite fields. Finite Fields and Their Applications, 2021, 70, 101797.	0.6	15
47	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
48	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
49	Generalized Plateaued Functions and Admissible (Plateaued) Functions. IEEE Transactions on Information Theory, 2017, 63, 6139-6148.	1.5	13
50	Threshold-Based Post-Quantum Secure Verifiable Multi-Secret Sharing for Distributed Storage Blockchain. Mathematics, 2020, 8, 2218.	1.1	13
51	On constructions of weightwise perfectly balanced Boolean functions. Cryptography and Communications, 2021, 13, 951-979.	0.9	13
52	Semi-bent Functions from Oval Polynomials. Lecture Notes in Computer Science, 2013, , 1-15.	1.0	13
53	Linear codes with one-dimensional hull associated with Gaussian sums. Cryptography and Communications, 2021, 13, 225-243.	0.9	12
54	On Hulls of Some Primitive BCH Codes and Self-Orthogonal Codes. IEEE Transactions on Information Theory, 2021, 67, 6442-6455.	1.5	12

#	ARTICLE	IF	CITATIONS
55	Survey on recent trends towards generalized differential and boomerang uniformities. <i>Cryptography and Communications</i> , 2022, 14, 691-735.	0.9	11
56	Constructions of Optimal Uniform Wide-Gap Frequency-Hopping Sequences. <i>IEEE Transactions on Information Theory</i> , 2022, 68, 692-700.	1.5	11
57	Results on Characterizations of Plateaued Functions in Arbitrary Characteristic. <i>Lecture Notes in Computer Science</i> , 2016, , 17-30.	1.0	10
58	On the dual of bent functions with $2^k$ Niho exponents. , 2011, , .		9
59	Several new classes of self-dual bent functions derived from involutions. <i>Cryptography and Communications</i> , 2019, 11, 1261-1273.	0.9	9
60	Further study on the maximum number of bent components of vectorial functions. <i>Designs, Codes, and Cryptography</i> , 2019, 87, 2597-2610.	1.0	9
61	Further Study of 2-to-1 Mappings Over $F_{2^n}$ . <i>IEEE Transactions on Information Theory</i> , 2021, 67, 3486-3496.	1.5	9
62	On Existence (Based on an Arithmetical Problem) and Constructions of Bent Functions. <i>Lecture Notes in Computer Science</i> , 2015, , 3-19.	1.0	9
63	Bent and Semi-bent Functions via Linear Translators. <i>Lecture Notes in Computer Science</i> , 2015, , 205-224.	1.0	9
64	On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. <i>Designs, Codes, and Cryptography</i> , 2022, 90, 1437-1461.	1.0	9
65	Dickson Polynomials, Hyperelliptic Curves and Hyper-bent Functions. <i>Lecture Notes in Computer Science</i> , 2012, , 40-52.	1.0	8
66	Semi-bent Functions with Multiple Trace Terms and Hyperelliptic Curves. <i>Lecture Notes in Computer Science</i> , 2012, , 18-36.	1.0	8
67	On the nonlinearity of S-boxes and linear codes. <i>Cryptography and Communications</i> , 2017, 9, 345-361.	0.9	8
68	On $q$ -ary plateaued functions over $F_{q^m}$ and their explicit characterizations. <i>European Journal of Combinatorics</i> , 2019, 80, 71-81.	0.5	8
69	Solving $x+x^{2^k}+\dots+x^{2^{ml}}=a$ over $\mathbb{F}_{2^n}$ . <i>Cryptography and Communications</i> , 2020, 12, 809-817.	0.9	8
70	New Bent Functions from Permutations and Linear Translators. <i>Lecture Notes in Computer Science</i> , 2017, , 282-297.	1.0	7
71	A class of narrow-sense BCH codes over $\mathbb{F}_q$ of length $\frac{q^m-1}{2}$ . <i>Designs, Codes, and Cryptography</i> , 2020, 88, 413-427.	1.0	7
72	Constructions of optimal locally recoverable codes via Dickson polynomials. <i>Designs, Codes, and Cryptography</i> , 2020, 88, 1759-1780.	1.0	7

#	ARTICLE	IF	CITATIONS
73	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
74	Generic Constructions of (Boolean and Vectorial) Bent Functions and Their Consequences. IEEE Transactions on Information Theory, 2022, 68, 2735-2751.	1.5	7
75	An efficient characterization of a family of hyper-bent functions with multiple trace terms. Journal of Mathematical Cryptology, 2013, 7, .	0.4	6
76	Bent functions linear on elements of some classical spreads and presemifields spreads. Cryptography and Communications, 2017, 9, 3-21.	0.9	6
77	On the $p$ -ary (cubic) bent and plateaued (vectorial) functions. Designs, Codes, and Cryptography, 2018, 86, 1865-1892.	1.0	6
78	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
79	Secondary constructions of (non)weakly regular plateaued functions over finite fields. Turkish Journal of Mathematics, 2021, 45, 2295-2306.	0.3	6
80	On the Link of Some Semi-bent Functions with Kloosterman Sums. Lecture Notes in Computer Science, 2011, , 263-272.	1.0	6
81	Explicit Characterizations for Plateaued-ness of $p$ -ary (Vectorial) Functions. Lecture Notes in Computer Science, 2017, , 328-345.	1.0	5
82	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
83	A direct proof of APN-ness of the Kasami functions. Designs, Codes, and Cryptography, 2021, 89, 441-446.	1.0	5
84	Complete solution over $\mathbb{F}_p$ of the equation $F(x) = \sum_{i=0}^{p-1} x^{i^2} = \sum_{i=0}^{p-1} x^{i^2} p$ of the equation $F(x) = \sum_{i=0}^{p-1} x^{i^2} = \sum_{i=0}^{p-1} x^{i^2} p$	0.6	5
85	Finite Fields and Their Applications, 2021, 76, 101902. Yet another variation on minimal linear codes. Advances in Mathematics of Communications, 2016, 10, 53-61.	0.4	5
86	On construction of bent functions involving symmetric functions and their duals. Advances in Mathematics of Communications, 2017, 11, 347-352.	0.4	5
87	Recent results on bent and hyper-bent functions and their link with some exponential sums. , 2010, , .		4
88	Hyper-bent functions via Dillon-like exponents. , 2012, , .		4
89	2-Correcting Lee Codes: (Quasi)-Perfect Spectral Conditions and Some Constructions. IEEE Transactions on Information Theory, 2018, 64, 3031-3041.	1.5	4
90	Multiple characters transforms and generalized Boolean functions. Cryptography and Communications, 2019, 11, 1247-1260.	0.9	4



#	ARTICLE	IF	CITATIONS
109	Statistical integral distinguisher with multi-structure and its application on AES-like ciphers. <i>Cryptography and Communications</i> , 2018, 10, 755-776.	0.9	2
110	Further study of 2-to-1 mappings over $F_{2^n}$ . , 2019, , .		2
111	Solving some affine equations over finite fields. <i>Finite Fields and Their Applications</i> , 2020, 68, 101746.	0.6	2
112	Cyclic Bent Functions and Their Applications in Sequences. <i>IEEE Transactions on Information Theory</i> , 2021, 67, 3473-3485.	1.5	2
113	Explicit constructions of bent functions from pseudo-planar functions. <i>Advances in Mathematics of Communications</i> , 2017, 11, 293-299.	0.4	2
114	Fast algebraic immunity of Boolean functions. <i>Advances in Mathematics of Communications</i> , 2017, 11, 373-377.	0.4	2
115	Bent Functions-Generalities. , 2016, , 69-91.		2
116	Constructions of Z-optimal Type-II quadriphase Z-complementary pairs. <i>Discrete Mathematics</i> , 2022, 345, 112685.	0.4	2
117	Constructions of two-dimensional Z-complementary array pairs with large ZCZ ratio. <i>Designs, Codes, and Cryptography</i> , 0, , 1.	1.0	2
118	Boolean Functions and Cryptography. , 2016, , 45-68.		1
119	A comparison of Carlet's second-order nonlinearity bounds. <i>International Journal of Computer Mathematics</i> , 2017, 94, 427-436.	1.0	1
120	Strongly Regular Graphs from Weakly Regular Plateaued Functions*. , 2019, , .		1
121	A proof of the Beierle-Kranz-Leander conjecture related to lightweight multiplication in $\mathbb{F}_{2^n}$ . <i>Designs, Codes, and Cryptography</i> , 2020, 88, 51-62.	1.0	1
122	Bent Vectorial Functions. , 2016, , 305-327.		1
123	Cryptanalysis of the AEAD and hash algorithm DryGASCON. <i>Cryptography and Communications</i> , 0, , 1.	0.9	1
124	New characterizations for the multi-output correlation-immune Boolean functions. <i>Discrete Mathematics</i> , 2020, 343, 112082.	0.4	1
125	Secret sharing schemes based on the dual of Golay codes. <i>Cryptography and Communications</i> , 2021, 13, 1025-1041.	0.9	1
126	On One-Dimensional Linear Minimal Codes Over Finite (Commutative) Rings. <i>IEEE Transactions on Information Theory</i> , 2022, 68, 2990-2998.	1.5	1

#	ARTICLE	IF	CITATIONS
127	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
128	Solving $X^2$ over Finite Fields and Their Applications, 2022, 83, 102086.	0.6	1
129	Generalized Witness Sets. , 2011, , .		0
130	Linear Codes from Bent, Semi-bent and Almost Bent Functions. , 2016, , 529-540.		0
131	Plateaued Functions: Generalities and Characterizations. , 2016, , 417-464.		0
132	On Plateaued Functions, Linear Structures and Permutation Polynomials. Lecture Notes in Computer Science, 2019, , 217-235.	1.0	0
133	On Good Polynomials over Finite Fields for Optimal Locally Recoverable Codes. Lecture Notes in Computer Science, 2019, , 257-268.	1.0	0
134	On generalized hyper-bent functions. Cryptography and Communications, 2020, 12, 455-468.	0.9	0
135	On correlation immune Boolean functions with minimum Hamming weight power of 2. IEEE Transactions on Information Theory, 2021, , 1-1.	1.5	0
136	More permutations and involutions for constructing bent functions. Cryptography and Communications, 2021, 13, 459-473.	0.9	0
137	Investigation for 8-bit SKINNY-like S-boxes, analysis and applications. Cryptography and Communications, 2021, 13, 617.	0.9	0
138	Preimages of $p$ -Linearized Polynomials over $\mathbb{F}_p$ . Cryptography and Communications, 0, , 1.	0.9	0
139	Bent Functions: Primary Constructions (Part I). , 2016, , 93-104.		0
140	Class $\mathcal{H}$ , Niho Bent Functions and o-Polynomials. , 2016, , 153-170.		0
141	Bent Functions and (Partial-)spreads. , 2016, , 345-385.		0
142	Bent Functions in Arbitrary Characteristic. , 2016, , 329-344.		0
143	Linear codes from support designs of ternary cyclic codes. Designs, Codes, and Cryptography, 2022, 90, 681.	1.0	0