

# Enes Pasalic

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/642937/publications.pdf>

Version: 2024-02-01

72  
papers

1,207  
citations

430754

18  
h-index

395590

33  
g-index

75  
all docs

75  
docs citations

75  
times ranked

295  
citing authors



#	ARTICLE	IF	CITATIONS
19	On the Maximum Number of Bent Components of Vectorial Functions. IEEE Transactions on Information Theory, 2018, 64, 403-411.	1.5	18
20	Full Characterization of Generalized Bent Functions as (Semi)-Bent Spaces, Their Dual, and the Gray Image. IEEE Transactions on Information Theory, 2018, 64, 5432-5440.	1.5	18
21	Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis. Lecture Notes in Computer Science, 2009, , 399-414.	1.0	18
22	Constructing Bent Functions Outside the Maiorana-McFarland Class Using a General Form of Rothaus. IEEE Transactions on Information Theory, 2017, 63, 5336-5349.	1.5	17
23	On multiple output bent functions. Information Processing Letters, 2012, 112, 811-815.	0.4	15
24	A Note on Generalized Bent Criteria for Boolean Functions. IEEE Transactions on Information Theory, 2013, 59, 3233-3236.	1.5	15
25	Large Sets of Orthogonal Sequences Suitable for Applications in CDMA Systems. IEEE Transactions on Information Theory, 2016, 62, 3757-3767.	1.5	15
26	Some results concerning cryptographically significant mappings over $GF(2^n)$ . Designs, Codes, and Cryptography, 2010, 57, 257-269.	1.0	14
27	New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions. Information Sciences, 2017, 415-416, 377-396.	4.0	12
28	Designing Plateaued Boolean Functions in Spectral Domain and Their Classification. IEEE Transactions on Information Theory, 2019, 65, 5865-5879.	1.5	12
29	Further analysis of bent functions from $C$ and $D$ which are provably outside or inside $\mathcal{PS}_m$	0.5	12
30	Highly Nonlinear Resilient Functions Through Disjoint Codes in Projective Spaces. Designs, Codes, and Cryptography, 2005, 37, 319-346.	1.0	11
31	An Analysis of the $\mathcal{C}$ Class of Bent Functions. Fundamenta Informaticae, 2016, 146, 271-292.	0.3	11
32	Generic Constructions of Five-Valued Spectra Boolean Functions. IEEE Transactions on Information Theory, 2019, 65, 7554-7565.	1.5	11
33	Vectorial Hyperbent Trace Functions From the $\mathcal{PS}_m$ Class—Their Exact Number and Specification. IEEE Transactions on Information Theory, 2014, 60, 4408-4413.	1.5	10
34	The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher. Lecture Notes in Computer Science, 2012, , 244-264.	1.0	9
35	Collisions for variants of the BLAKE hash function. Information Processing Letters, 2010, 110, 585-590.	0.4	8
36	Probabilistic Versus Deterministic Algebraic Cryptanalysis—A Performance Comparison. IEEE Transactions on Information Theory, 2009, 55, 5233-5240.	1.5	7

#	ARTICLE	IF	CITATIONS
37	Characterization of Basic 5-Value Spectrum Functions Through Walsh-Hadamard Transform. IEEE Transactions on Information Theory, 2021, 67, 1038-1053.	1.5	7
38	On the Construction of Cryptographically Significant Boolean Functions Using Objects in Projective Geometry Spaces. IEEE Transactions on Information Theory, 2012, 58, 6681-6693.	1.5	5
39	Guess and Determine Attacks on Filter Generators Revisited. IEEE Transactions on Information Theory, 2012, 58, 2530-2539.	1.5	5
40	A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation. Cryptography and Communications, 2012, 4, 25-45.	0.9	5
41	Construction methods for generalized bent functions. Discrete Applied Mathematics, 2018, 238, 14-23.	0.5	5
42	On Cryptographically Significant Mappings over $GF(2^n)$ . Lecture Notes in Computer Science, 2008, , 189-204.	1.0	5
43	Phase orthogonal sequence sets for (QS)CDMA communications. Designs, Codes, and Cryptography, 2022, 90, 1139-1156.	1.0	5
44	A New Correlation Attack on Nonlinear Combining Generators. IEEE Transactions on Information Theory, 2011, 57, 6321-6331.	1.5	4
45	Infinite classes of vectorial plateaued functions, permutations and complete permutations. Discrete Applied Mathematics, 2016, 215, 177-184.	0.5	4
46	Efficient probabilistic algorithm for estimating the algebraic properties of Boolean functions for large $n$ . Information Sciences, 2017, 402, 91-104.	4.0	4
47	Construction of resilient $S$ -boxes with higher-dimensional vectorial outputs and strictly almost optimal non-linearity. IET Information Security, 2017, 11, 199-203.	1.1	4
48	New second-order threshold implementation of AES. IET Information Security, 2019, 13, 117-124.	1.1	4
49	Several classes of minimal binary linear codes violating the Ashikhmin-Barg bound. Cryptography and Communications, 2021, 13, 637-659.	0.9	4
50	Constructing new superclasses of bent functions from known ones. Cryptography and Communications, 2022, 14, 1229-1256.	0.9	4
51	On upper bounds on algebraic immunity of some PS and Niho bent functions. , 2013, , .		3
52	The higher-order meet-in-the-middle attack and its application to the Camellia block cipher. Theoretical Computer Science, 2014, 527, 102-122.	0.5	3
53	On cross-correlation properties of $S$ -boxes and their design using semi-bent functions. Security and Communication Networks, 2015, 8, 790-800.	1.0	3
54	A note on nonexistence of vectorial bent functions with binomial trace representation in the $\langle \text{mml:math altimg="si1.gif" overflow="scroll" xmlns:xocs="http://www.elsevier.com/xml/xocs/dtd" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://www.elsevier.com/xml/ja/dtd" xmlns:ja="http://www.elsevier.com/xml/ja/dtd" xmlns:mml="http://www.w3.org/1998/Math/MathML" xmlns:tb="http://www.elsevier.com/xml/common/table/dtd" xmlns:sb="http://www.elsevier.com/} \rangle$ Infor	0.4	3

#	ARTICLE	IF	CITATIONS
55	Efficient implementation of generalized Maiorana-McFarland class of cryptographic functions. Journal of Cryptographic Engineering, 2017, 7, 287-295.	1.5	3
56	On generalized bent functions with Dillon's exponents. Information Processing Letters, 2014, 114, 222-227.	0.4	2
57	On derivatives of polynomials over finite fields through integration. Discrete Applied Mathematics, 2017, 217, 294-303.	0.5	2
58	Wide minimal binary linear codes from the general Maiorana-McFarland class. Designs, Codes, and Cryptography, 2021, 89, 1485-1507.	1.0	2
59	Generalized bent functions -sufficient conditions and related constructions. Advances in Mathematics of Communications, 2017, 11, 549-566.	0.4	2
60	Further study on constructing bent functions outside the completed Maiorana-McFarland class. IET Information Security, 2020, 14, 654-660.	1.1	2
61	Minimal binary linear codes: a general framework based on bent concatenation. Designs, Codes, and Cryptography, 2022, 90, 1289-1318.	1.0	2
62	On the approximation of S-boxes via Maiorana-McFarland functions. IET Information Security, 2013, 7, 134-143.	1.1	1
63	An analysis of root functions - A subclass of the Impossible Class of Faulty Functions (ICFF). Discrete Applied Mathematics, 2017, 222, 1-13.	0.5	1
64	Optimizing the Placement of Tap Positions. Lecture Notes in Computer Science, 2015, , 15-30.	1.0	1
65	On algebraic properties of S-boxes designed by means of disjoint linear codes. International Journal of Computer Mathematics, 2016, 93, 55-66.	1.0	0
66	A note on non-splitting $\langle m, m \rangle$ .  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" xmlns:tb="http://www.elsevier.com/xml/common/table/dtd" xmlns:sb="http://www.elsevier.com/xml/common/struct-bib/dtd" xmlns:ce="http://www.elsevier.com/x	0.4	0
67	On derivatives of planar mappings and their connections to complete mappings. Discrete Applied Mathematics, 2018, 250, 285-290.	0.5	0
68	Guess and determine cryptanalysis with variable sampling and its applications. IET Information Security, 2019, 13, 559-569.	1.1	0
69	Correction to "Large sets of orthogonal sequences suitable for applications in cdma systems" [Jun 16 3757-3767]. IEEE Transactions on Information Theory, 2019, 65, 1318-1318.	1.5	0
70	Bent functions from nonlinear permutations and conversely. Cryptography and Communications, 2019, 11, 207-225.	0.9	0
71	Constructions of balanced Boolean functions on even number of variables with maximum absolute value in autocorrelation spectra $\leq 2\sqrt{n}$ . Information Sciences, 2021, 575, 437-453.	4.0	0
72	Three classes of balanced vectorial semi-bent functions. Designs, Codes, and Cryptography, 2021, 89, 2697.	1.0	0