# Enes Pasalic

List of Publications by Year
in descending order

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

Version: 2024-02-01

| 72 | 1,207 | 430754 | 395590 |
|---|---|---|---|
| papers | citations | 18 h-index | 33 g-index |

| 75 | 75 | 75 | 295 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Phase orthogonal sequence sets for (QS)CDMA communications. Designs, Codes, and Cryptography, 2022, 90, 1139-1156. | 1.0 | 5 |
| 2 | Constructing new superclasses of bent functions from known ones. Cryptography and Communications, 2022, 14, 1229-1256. | 0.9 | 4 |
| 3 | Minimal binary linear codes: a general framework based on bent concatenation. Designs, Codes, and Cryptography, 2022, 90, 1289-1318. | 1.0 | 2 |
| 4 | Characterization of Basic 5-Value Spectrum Functions Through Walsh-Hadamard Transform. IEEE Transactions on Information Theory, 2021, 67, 1038-1053. | 1.5 | 7 |
| 5 | Wide minimal binary linear codes from the general Maioranaâ€“McFarland class. Designs, Codes, and Cryptography, 2021, 89, 1485-1507. | 1.0 | 2 |
| 6 | Several classes of minimal binary linear codes violating the Ashikhmin-Barg bound. Cryptography and Communications, 2021, 13, 637-659. | 0.9 | 4 |
| 7 | Constructions of balanced Boolean functions on even number of variables with maximum absolute value in autocorrelation spectra <2n2â˜†. Information Sciences, 2021, 575, 437-453. | 4.0 | 0 |
| 8 | Three classes of balanced vectorial semi-bent functions. Designs, Codes, and Cryptography, 2021, 89, 2697. | 1.0 | 0 |
| 9 | Further analysis of bent functions from <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e20" altimg="si29.svg"><mml:mi mathvariant="script">C</mml:mi></mml:math> and <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e25" altimg="si30.svg"><mml:mi mathvariant="script">D</mml:mi></mml:math> which are provably outside or inside <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e30" alt | 0.5 | 12 |
| 10 | Further study on constructing bent functions outside the completed Maioranaâ€“McFarland class. IET Information Security, 2020, 14, 654-660. | 1.1 | 2 |
| 11 | Designing Plateaued Boolean Functions in Spectral Domain and Their Classification. IEEE Transactions on Information Theory, 2019, 65, 5865-5879. | 1.5 | 12 |
| 12 | Generic Constructions of Five-Valued Spectra Boolean Functions. IEEE Transactions on Information Theory, 2019, 65, 7554-7565. | 1.5 | 11 |
| 13 | New secondâ€order threshold implementation of AES. IET Information Security, 2019, 13, 117-124. | 1.1 | 4 |
| 14 | Guess and determine cryptanalysis with variable sampling and its applications. IET Information Security, 2019, 13, 559-569. | 1.1 | 0 |
| 15 | Correction to â€œlarge sets of orthogonal sequences suitable for applications in cdma systemsâ€•[jun 16 3757-3767]. IEEE Transactions on Information Theory, 2019, 65, 1318-1318. | 1.5 | 0 |
| 16 | Bent functions from nonlinear permutations and conversely. Cryptography and Communications, 2019, 11, 207-225. | 0.9 | 0 |
| 17 | Large Sets of Disjoint Spectra Plateaued Functions Inequivalent to Partially Linear Functions. IEEE Transactions on Information Theory, 2018, 64, 2987-2999. | 1.5 | 19 |
| 18 | Construction methods for generalized bent functions. Discrete Applied Mathematics, 2018, 238, 14-23. | 0.5 | 5 |

| # | 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 | On derivatives of planar mappings and their connections to complete mappings. Discrete Applied Mathematics, 2018, 250, 285-290. | 0.5 | 0 |
| 21 | 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 |
| 22 | On derivatives of polynomials over finite fields through integration. Discrete Applied Mathematics, 2017, 217, 294-303. | 0.5 | 2 |
| 23 | A note on multi-splitting <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/xml/common/struct-bib/dtd" xmlns:ce="http://www.elsevier.com/x | 0.4 | 0 |
| 24 | Efficient probabilistic algorithm for estimating the algebraic properties of Boolean functions for large n. Information Sciences, 2017, 402, 91-104. | 4.0 | 4 |
| 25 | An analysis of root functionsâ€"A subclass of the Impossible Class of Faulty Functions (ICFF). Discrete Applied Mathematics, 2017, 222, 1-13. | 0.5 | 1 |
| 26 | Permutations via linear translators. Finite Fields and Their Applications, 2017, 45, 19-42. | 0.6 | 19 |
| 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 | Constructing Bent Functions Outside the Maioranaâ€"McFarland Class Using a General Form of Rothaus. IEEE Transactions on Information Theory, 2017, 63, 5336-5349. | 1.5 | 17 |
| 29 | Construction of resilient Sâ€boxes with higherâ€dimensional vectorial outputs and strictly almost optimal nonâ€linearity. IET Information Security, 2017, 11, 199-203. | 1.1 | 4 |
| 30 | Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria. Information Sciences, 2017, 376, 21-30. | 4.0 | 22 |
| 31 | Efficient implementation of generalized Maioranaâ€"McFarland class of cryptographic functions. Journal of Cryptographic Engineering, 2017, 7, 287-295. | 1.5 | 3 |
| 32 | Generalized bent functions -sufficient conditions and related constructions. Advances in Mathematics of Communications, 2017, 11, 549-566. | 0.4 | 2 |
| 33 | An Analysis of the ? Class of Bent Functions. Fundamenta Informaticae, 2016, 146, 271-292. | 0.3 | 11 |
| 34 | Large Sets of Orthogonal Sequences Suitable for Applications in CDMA Systems. IEEE Transactions on Information Theory, 2016, 62, 3757-3767. | 1.5 | 15 |
| 35 | Infinite classes of vectorial plateaued functions, permutations and complete permutations. Discrete Applied Mathematics, 2016, 215, 177-184. | 0.5 | 4 |
| 36 | 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 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | On crossâ€correlation properties of Sâ€boxes and their design using semiâ€bent functions. Security and Communication Networks, 2015, 8, 790-800. | 1.0 | 3 |
| 38 | Constructions of Bentâ€"Negabent Functions and Their Relation to the Completed Maioranaâ€"McFarland Class. IEEE Transactions on Information Theory, 2015, 61, 1496-1506. | 1.5 | 25 |
| 39 | Generalized Bent Functions - Some General Construction Methods and Related Necessary and Sufficient Conditions. Cryptography and Communications, 2015, 7, 469-483. | 0.9 | 19 |
| 40 | A note on nonexistence of vectorial bent functions with binomial trace representation in the <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/. Infor | 0.4 | 3 |
| 41 | Optimizing the Placement of Tap Positions. Lecture Notes in Computer Science, 2015, , 15-30. | 1.0 | 1 |
| 42 | 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 |
| 43 | Constructions of Resilient S-Boxes With Strictly Almost Optimal Nonlinearity Through Disjoint Linear Codes. IEEE Transactions on Information Theory, 2014, 60, 1638-1651. | 1.5 | 30 |
| 44 | Vectorial Bent Functions From Multiple Terms Trace Functions. IEEE Transactions on Information Theory, 2014, 60, 1337-1347. | 1.5 | 23 |
| 45 | Highly Nonlinear Balanced S-Boxes With Good Differential Properties. IEEE Transactions on Information Theory, 2014, 60, 7970-7979. | 1.5 | 35 |
| 46 | Generalized Maioranaâ€"McFarland Construction of Resilient Boolean Functions With High Nonlinearity and Good Algebraic Properties. IEEE Transactions on Information Theory, 2014, 60, 6681-6695. | 1.5 | 45 |
| 47 | Vectorial Hyperbent Trace Functions From the (mathcal {PS}_{m ap}) Classâ€"Their Exact Number and Specification. IEEE Transactions on Information Theory, 2014, 60, 4408-4413. | 1.5 | 10 |
| 48 | On generalized bent functions with DillonÊ¼s exponents. Information Processing Letters, 2014, 114, 222-227. | 0.4 | 2 |
| 49 | A note on complete polynomials over finite fields and their applications in cryptography. Finite Fields and Their Applications, 2014, 25, 306-315. | 0.6 | 33 |
| 50 | On upper bounds on algebraic immunity of some PS<inf>ap</inf> and Niho bent functions. , 2013, , . | | 3 |
| 51 | A Note on Generalized Bent Criteria for Boolean Functions. IEEE Transactions on Information Theory, 2013, 59, 3233-3236. | 1.5 | 15 |
| 52 | On the approximation of Sâ€boxes via Maioranaâ€"McFarland functions. IET Information Security, 2013, 7, 134-143. | 1.1 | 1 |
| 53 | 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 |
| 54 | On multiple output bent functions. Information Processing Letters, 2012, 112, 811-815. | 0.4 | 15 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | Guess and Determine Attacks on Filter Generatorsâ€”Revisited. IEEE Transactions on Information Theory, 2012, 58, 2530-2539. | 1.5 | 5 |
| 56 | A design of Boolean functions resistant to (fast) algebraic cryptanalysis with efficient implementation. Cryptography and Communications, 2012, 4, 25-45. | 0.9 | 5 |
| 57 | 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 |
| 58 | A New Correlation Attack on Nonlinear Combining Generators. IEEE Transactions on Information Theory, 2011, 57, 6321-6331. | 1.5 | 4 |
| 59 | Some results concerning cryptographically significant mappings over GF(2 n ). Designs, Codes, and Cryptography, 2010, 57, 257-269. | 1.0 | 14 |
| 60 | Collisions for variants of the BLAKE hash function. Information Processing Letters, 2010, 110, 585-590. | 0.4 | 8 |
| 61 | On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers. IEEE Transactions on Information Theory, 2009, 55, 3398-3406. | 1.5 | 21 |
| 62 | Probabilistic Versus Deterministic Algebraic Cryptanalysisâ€”A Performance Comparison. IEEE Transactions on Information Theory, 2009, 55, 5233-5240. | 1.5 | 7 |
| 63 | Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis. Lecture Notes in Computer Science, 2009, , 399-414. | 1.0 | 18 |
| 64 | On Cryptographically Significant Mappings over GF(2 n ). Lecture Notes in Computer Science, 2008, , 189-204. | 1.0 | 5 |
| 65 | A Maioranaâ€“McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity <mml:math 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" xmlns:tb="http://www.elsevier.com/xml/common/table/dtd" xmlns:sb="http://... Discrete Applied Mathemat... | 0.5 | 18 |
| 66 | Maioranaâ€“McFarland Class: Degree Optimization and Algebraic Properties. IEEE Transactions on Information Theory, 2006, 52, 4581-4594. | 1.5 | 21 |
| 67 | On Bent and Semi-Bent Quadratic Boolean Functions. IEEE Transactions on Information Theory, 2005, 51, 4286-4298. | 1.5 | 99 |
| 68 | Highly Nonlinear Resilient Functions Through Disjoint Codes in Projective Spaces. Designs, Codes, and Cryptography, 2005, 37, 319-346. | 1.0 | 11 |
| 69 | Algebraic Attacks and Decomposition of Boolean Functions. Lecture Notes in Computer Science, 2004, , 474-491. | 1.0 | 270 |
| 70 | A construction of resilient functions with high nonlinearity. IEEE Transactions on Information Theory, 2003, 49, 494-501. | 1.5 | 48 |
| 71 | Linear codes in generalized construction of resilient functions with very high nonlinearity. IEEE Transactions on Information Theory, 2002, 48, 2182-2191. | 1.5 | 35 |
| 72 | New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity. Electronic Notes in Discrete Mathematics, 2001, 6, 158-167. | 0.4 | 58 |