Claude Carlet

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5324085/publications.pdf

Version: 2024-02-01

187
papers

6,717
citations

87723

38
h-index

106150

65
g-index

195
all docs

195
docs citations

195
times ranked

1105
citing authors

#	Article	IF	Citations
1	Revisiting some results on APN and algebraic immune functions. Advances in Mathematics of Communications, 2023, 17, 1012-1026.	0.4	2
2	Spectral approach to process the (multivariate) high-order template attack against any masking scheme. Journal of Cryptographic Engineering, 2022, 12, 75-93.	1.5	2
3	A Complete Study of Two Classes of Boolean Functions: Direct Sums of Monomials and Threshold Functions. IEEE Transactions on Information Theory, 2022, 68, 3404-3425.	1.5	10
4	A Wide Class of Boolean Functions Generalizing the Hidden Weight Bit Function. IEEE Transactions on Information Theory, 2022, 68, 1355-1368.	1.5	2
5	On Two Fundamental Problems on APN Power Functions. IEEE Transactions on Information Theory, 2022, 68, 3389-3403.	1.5	7
6	Parameterization of Boolean functions by vectorial functions and associated constructions. Advances in Mathematics of Communications, 2022, .	0.4	2
7	Information Leakage in Code-Based Masking: A Systematic Evaluation by Higher-Order Attacks. IEEE Transactions on Information Forensics and Security, 2022, 17, 1624-1638.	4.5	2
8	A further study of quadratic APN permutations in dimension nine. Finite Fields and Their Applications, 2022, 81, 102049.	0.6	5
9	Expressing the minimum distance, weight distribution and covering radius of codes by means of the algebraic and numerical normal forms of their indicators. Advances in Mathematics of Communications, 2022, 16, 693-707.	0.4	1
10	Side-Channel Information Leakage of Code-Based Masked Implementations. , 2022, , .		0
11	Detecting faults in inner product masking scheme. Journal of Cryptographic Engineering, 2021, 11, 119-133.	1.5	3
12	Optimizing Inner Product Masking Scheme by a Coding Theory Approach. IEEE Transactions on Information Forensics and Security, 2021, 16, 220-235.	4.5	18
13	Intrinsic Resiliency of S-Boxes Against Side-Channel Attacksâ€“Best and Worst Scenarios. IEEE Transactions on Information Forensics and Security, 2021, 16, 203-218.	4.5	9
14	Generalized isotopic shift construction for APN functions. Designs, Codes, and Cryptography, 2021, 89, 19-32.	1.0	9
15	A direct proof of APN-ness of the Kasami functions. Designs, Codes, and Cryptography, 2021, 89, 441-446.	1.0	5
16	Bounds on the Nonlinearity of Differentially Uniform Functions by Means of Their Image Set Size, and on Their Distance to Affine Functions. IEEE Transactions on Information Theory, 2021, 67, 8325-8334.	1.5	5
17	Categorizing all linear codes of IPM over ${mathbb {F}}_{2^{8}}$. Cryptography and Communications, 2021, 13, 527-542.	0.9	0
18	Evolutionary algorithms-assisted construction of cryptographic boolean functions. , 2021, , .		6

#	Article	IF	Citations
19	Relation between o-equivalence and EA-equivalence for Niho bent functions. Finite Fields and Their Applications, 2021, 72, 101834.	0.6	0
20	Cumulant Expansion of Mutual Information for Quantifying Leakage of a Protected Secret. , 2021, , .		0
21	On the Properties of the Boolean Functions Associated to the Differential Spectrum of General APN Functions and Their Consequences. IEEE Transactions on Information Theory, 2021, 67, 6926-6939.	1.5	2
22	Linear Programming Bounds on the Kissing Number of q-ary Codes. , 2021, , .		3
23	Reducing Aging Impacts in Digital Sensors via Run-Time Calibration. Journal of Electronic Testing: Theory and Applications (JETTA), 2021, 37, 653-673.	0.9	4
24	The Fifth International Studentsâ€™ Olympiad in cryptographyâ€”NSUCRYPTO: Problems and their solutions. Cryptologia, 2020, 44, 223-256.	0.4	4
25	Graph Indicators of Vectorial Functions and Bounds on the Algebraic Degree of Composite Functions. IEEE Transactions on Information Theory, 2020, 66, 7702-7716.	1.5	5
26	Handling Vectorial Functions by Means of Their Graph Indicators. IEEE Transactions on Information Theory, 2020, 66, 6324-6339.	1.5	7
27	On the Distance Between APN Functions. IEEE Transactions on Information Theory, 2020, 66, 5742-5753.	1.5	9
28	Constructing APN Functions Through Isotopic Shifts. IEEE Transactions on Information Theory, 2020, 66, 5299-5309.	1.5	26
29	New Characterization and Parametrization of LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 39-49.	1.5	40
30	On APN exponents, characterizations of differentially uniform functions by the Walsh transform, and related cyclic-difference-set-like structures. Designs, Codes, and Cryptography, 2019, 87, 203-224.	1.0	6
31	Linear codes with small hulls in semi-primitive case. Designs, Codes, and Cryptography, 2019, 87, 3063-3075.	1.0	17
32	Some (almost) optimally extendable linear codes. Designs, Codes, and Cryptography, 2019, 87, 2813-2834.	1.0	3
33	On the Derivative Imbalance and Ambiguity of Functions. IEEE Transactions on Information Theory, 2019, 65, 5833-5845.	1.5	4
34	Polynomial direct sum masking to protect against both SCA and FIA. Journal of Cryptographic Engineering, 2019, 9, 303-312.	1.5	6
35	On $sigma$ -LCD Codes. IEEE Transactions on Information Theory, 2019, 65, 1694-1704.	1.5	29
36	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.	1.0	1

#	Article	IF	Citations
37	Confused yet Successful:. Lecture Notes in Computer Science, 2019, , 533-553.	1.0	1
38	Constructing Low-Weight $d$ th-Order Correlation-Immune Boolean Functions Through the Fourier-Hadamard Transform. IEEE Transactions on Information Theory, 2018, 64, 2969-2978.	1.5	14
39	Euclidean and Hermitian LCD MDS codes. Designs, Codes, and Cryptography, 2018, 86, 2605-2618.	1.0	75
40	Linear Codes Over $mathbb F_q$ Are Equivalent to LCD Codes for $q&gt;3$. IEEE Transactions on Information Theory, 2018, 64, 3010-3017.	1.5	114
41	On Linear Complementary Pairs of Codes. IEEE Transactions on Information Theory, 2018, 64, 6583-6589.	1.5	32
42	Connecting and Improving Direct Sum Masking and Inner Product Masking. Lecture Notes in Computer Science, 2018, , 123-141.	1.0	10
43	Statistical properties of side-channel and fault injection attacks using coding theory. Cryptography and Communications, 2018, 10, 909-933.	0.9	21
44	A new concatenated type construction for LCD codes and isometry codes. Discrete Mathematics, 2018, 341, 830-835.	0.4	10
45	Characterizations of the Differential Uniformity of Vectorial Functions by the Walsh Transform. IEEE Transactions on Information Theory, 2018, 64, 6443-6453.	1.5	26
46	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
47	On the nonlinearity of monotone Boolean functions. Cryptography and Communications, 2018, 10, 1051-1061.	0.9	5
48	On the optimality and practicability of mutual information analysis in some scenarios. Cryptography and Communications, 2018, 10, 101-121.	0.9	13
49	Componentwise APNness, Walsh uniformity of APN functions, and cyclic-additive difference sets. Finite Fields and Their Applications, 2018, 53, 226-253.	0.6	5
50	On Upper Bounds for Algebraic Degrees of APN Functions. IEEE Transactions on Information Theory, 2018, 64, 4399-4411.	1.5	16
51	Impact of Aging on the Reliability of Delay PUFs. Journal of Electronic Testing: Theory and Applications (JETTA), 2018, 34, 571-586.	0.9	19
52	Physical Security Versus Masking Schemes. , 2018, , 269-284.		1
53	Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions. Lecture Notes in Computer Science, 2017, , 328-345.	1.0	5
54	Binary linear codes from vectorial boolean functions and their weight distribution. Discrete Mathematics, 2017, 340, 3055-3072.	0.4	13

#	Article	IF	Citations
55	Construction of Highly Nonlinear 1-Resilient Boolean Functions with Optimal Algebraic Immunity and Provably High Fast Algebraic Immunity. IEEE Transactions on Information Theory, 2017, , 1-1.	1.5	14
56	Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience. Lecture Notes in Computer Science, 2017, , 393-414.	1.0	16
57	Codes for Side-Channel Attacks and Protections. Lecture Notes in Computer Science, 2017, , 35-55.	1.0	8
58	Three basic questions on Boolean functions. Advances in Mathematics of Communications, 2017, 11, 837-855.	0.4	0
59	Evolutionary Algorithms for Boolean Functions in Diverse Domains of Cryptography. Evolutionary Computation, 2016, 24, 667-694.	2.3	38
60	On the (non-)existence of APN (n, n)-functions of algebraic degree n. , 2016, , .		2
61	Cryptographic properties of monotone Boolean functions. Journal of Mathematical Cryptology, 2016, 10, 1-14.	0.4	8
62	New secondary constructions of Bent functions. Applicable Algebra in Engineering, Communications and Computing, 2016, 27, 413-434.	0.3	18
63	Quadratic zero-difference balanced functions, APN functions and strongly regular graphs. Designs, Codes, and Cryptography, 2016, 78, 629-654.	1.0	7
64	Four decades of research on bent functions. Designs, Codes, and Cryptography, 2016, 78, 5-50.	1.0	156
65	Univariate Niho Bent Functions From o-Polynomials. IEEE Transactions on Information Theory, 2016, 62, 2254-2265.	1.5	9
66	Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. Lecture Notes in Computer Science, 2016, , 311-343.	1.0	78
67	Complementary dual codes for counter-measures to side-channel attacks. Advances in Mathematics of Communications, 2016, 10, 131-150.	0.4	131
68	Differentially 4-uniform bijections by permuting the inverse function. Designs, Codes, and Cryptography, 2015, 77, 117-141.	1.0	52
69	Algebraic Decomposition for Probing Security. Lecture Notes in Computer Science, 2015, , 742-763.	1.0	25
70	Correlation Immunity of Boolean Functions. , 2015, , .		15
71	Boolean and Vectorial Plateaued Functions and APN Functions. IEEE Transactions on Information Theory, 2015, 61, 6272-6289.	1.5	49
72	S-boxes, Boolean Functions and Codes for the Resistance of Block Ciphers to Cryptographic Attacks, with or without Side Channels. Lecture Notes in Computer Science, 2015, , 151-171.	1.0	2

#	Article	IF	Citations
73	Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. , 2015, , .		43
74	On the Properties of Vectorial Functions with Plateaued Components and Their Consequences on APN Functions. Lecture Notes in Computer Science, 2015, , 63-73.	1.0	6
75	Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks. Designs, Codes, and Cryptography, 2015, 76, 279-305.	1.0	18
76	Enhanced Boolean functions suitable for the filter model of pseudo-random generator. Designs, Codes, and Cryptography, 2015, 76, 571-587.	1.0	9
77	Open Questions on Nonlinearity and on APN Functions. Lecture Notes in Computer Science, 2015, , 83-107.	1.0	18
78	A Key to Success. Lecture Notes in Computer Science, 2015, , 270-290.	1.0	14
79	Evolutionary Approach for Finding Correlation Immune Boolean Functions of Order t with Minimal Hamming Weight. Lecture Notes in Computer Science, 2015, , 71-82.	1.0	16
80	A new construction of differentially 4-uniform $(n,n-1)$-functions. Advances in Mathematics of Communications, 2015, 9, 541-565.	0.4	5
81	A CLASS OF 1-RESILIENT BOOLEAN FUNCTIONS WITH OPTIMAL ALGEBRAIC IMMUNITY AND GOOD BEHAVIOR AGAINST FAST ALGEBRAIC ATTACKS. International Journal of Foundations of Computer Science, 2014, 25, 763-780.	0.8	11
82	Niho bent functions from quadratic o-monomials. , 2014, , .		7
83	Leakage squeezing: Optimal implementation and security evaluation. Journal of Mathematical Cryptology, 2014, 8, 249-295.	0.4	13
84	Achieving side-channel high-order correlation immunity with leakage squeezing. Journal of Cryptographic Engineering, 2014, 4, 107-121.	1.5	20
85	Multiply Constant-Weight Codes and the Reliability of Loop Physically Unclonable Functions. IEEE Transactions on Information Theory, 2014, 60, 7026-7034.	1.5	23
86	Higher-Order CIS Codes. IEEE Transactions on Information Theory, 2014, 60, 5283-5295.	1.5	7
87	A secondary construction and a transformation on rotation symmetric functions, and their action on bent and semi-bent functions. Journal of Combinatorial Theory - Series A, 2014, 127, 161-175.	0.5	55
88	Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions. Information Sciences, 2014, 283, 94-106.	4.0	27
89	Cryptographic properties of the hidden weighted bit function. Discrete Applied Mathematics, 2014, 174, 1-10.	0.5	17
90	Detecting Hidden Leakages. Lecture Notes in Computer Science, 2014, , 324-342.	1.0	37

#	Article	IF	Citations
91	A Theoretical Study of Kolmogorov-Smirnov Distinguishers. Lecture Notes in Computer Science, 2014, , 9-28.	1.0	18
92	Open Problems on Binary Bent Functions. , 2014, , 203-241.		16
93	Results on Constructions of Rotation Symmetric Bent and Semi-bent Functions. Lecture Notes in Computer Science, 2014, , 21-33.	1.0	15
94	Orthogonal Direct Sum Masking. Lecture Notes in Computer Science, 2014, , 40-56.	1.0	55
95	Masks Will Fall Off. Lecture Notes in Computer Science, 2014, , 344-365.	1.0	25
96	More constructions of APN and differentially 4-uniform functions by concatenation. Science China Mathematics, 2013, 56, 1373-1384.	0.8	16
97	A Survey on Nonlinear Boolean Functions with Optimal Algebraic Immunity Suitable for Stream Ciphers. Vietnam Journal of Mathematics, 2013, 41, 527-541.	0.4	7
98	Highly Nonlinear Boolean Functions With Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks. IEEE Transactions on Information Theory, 2013, 59, 653-664.	1.5	79
99	On the second-order nonlinearities of some bent functions. Information Sciences, 2013, 223, 322-330.	4.0	16
100	A low-entropy first-degree secure provable masking scheme for resource-constrained devices. , 2013, , .		13
101	Correlation-Immune Boolean Functions for Leakage Squeezing and Rotating S-Box Masking against Side Channel Attacks. Lecture Notes in Computer Science, 2013, , 70-74.	1.0	8
102	Asymptotic lower bound on the algebraic immunity of random balanced multi-output Boolean functions. Advances in Mathematics of Communications, 2013, 7, 197-217.	0.4	1
103	RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs. , 2012, , .		116
104	Generalized bent functions and their relation to Maiorana-McFarland class. , 2012, , .		13
105	Further Results on Niho Bent Functions. IEEE Transactions on Information Theory, 2012, 58, 6979-6985.	1.5	38
106	A New Class of Codes for Boolean Masking of Cryptographic Computations. IEEE Transactions on Information Theory, 2012, 58, 6000-6011.	1.5	20
107	PICARO â€“ A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. Lecture Notes in Computer Science, 2012, , 311-328.	1.0	60
108	Analysis of the algebraic side channel attack. Journal of Cryptographic Engineering, 2012, 2, 45-62.	1.5	23

#	Article	IF	Citations
109	Portability of templates. Journal of Cryptographic Engineering, 2012, 2, 63-74.	1.5	32
110	On Semibent Boolean Functions. IEEE Transactions on Information Theory, 2012, 58, 3287-3292.	1.5	36
111	Constructions of Quadratic and Cubic Rotation Symmetric Bent Functions. IEEE Transactions on Information Theory, 2012, 58, 4908-4913.	1.5	47
112	Optimal First-Order Masking with Linear and Non-linear Bijections. Lecture Notes in Computer Science, 2012, , 360-377.	1.0	12
113	Higher-Order Masking Schemes for S-Boxes. Lecture Notes in Computer Science, 2012, , 366-384.	1.0	84
114	Comparison between Side-Channel Analysis Distinguishers. Lecture Notes in Computer Science, 2012, , 331-340.	1.0	16
115	Leakage Squeezing of Order Two. Lecture Notes in Computer Science, 2012, , 120-139.	1.0	25
116	Bent functions on a Galois ring and systematic authentication codes. Advances in Mathematics of Communications, 2012, 6, 249-258.	0.4	6
117	Secondary constructions of bent functions and their enforcement. Advances in Mathematics of Communications, 2012, 6, 305-314.	0.4	33
118	On bent functions associated to AB functions. , 2011, , .		11
119	More Balanced Boolean Functions With Optimal Algebraic Immunity and Good Nonlinearity and Resistance to Fast Algebraic Attacks. IEEE Transactions on Information Theory, 2011, 57, 6310-6320.	1.5	72
120	Comments on "Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials. IEEE Transactions on Information Theory, 2011, 57, 4852-4853.	1.5	18
121	CCZ-equivalence of bent vectorial functions and related constructions. Designs, Codes, and Cryptography, 2011, 59, 69-87.	1.0	19
122	Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. Designs, Codes, and Cryptography, 2011, 59, 89-109.	1.0	54
123	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
124	On the dual of bent functions with 2&lt;sup&gt;r&lt;/sup&gt; Niho exponents. , 2011, , .		9
125	MORE VECTORIAL BOOLEAN FUNCTIONS WITH UNBOUNDED NONLINEARITY PROFILE. International Journal of Foundations of Computer Science, 2011, 22, 1259-1269.	0.8	11
126	Leakage Squeezing Countermeasure against High-Order Attacks. Lecture Notes in Computer Science, 2011, , 208-223.	1.0	27

#	Article	IF	Citations
127	On Known and New Differentially Uniform Functions. Lecture Notes in Computer Science, 2011, , 1-15.	1.0	30
128	Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks. Lecture Notes in Computer Science, 2011, , 22-39.	1.0	21
129	Vectorial Boolean Functions for Cryptography. , 2010, , 398-470.		242
130	Self-dual bent functions. International Journal of Information and Coding Theory, 2010, 1, 384.	0.3	35
131	Boolean Functions for Cryptography and Error-Correcting Codes. , 2010, , 257-397.		464
132	On the construction of bent vectorial functions. International Journal of Information and Coding Theory, 2010, 1, 133.	0.3	16
133	On the Higher Order Nonlinearities of Boolean Functions and S-boxes. , 2009, , .		4
134	Further properties of several classes of Boolean functions with optimum algebraic immunity. Designs, Codes, and Cryptography, 2009, 52, 303-338.	1.0	82
135	Constructing new APN functions from known ones. Finite Fields and Their Applications, 2009, 15, 150-159.	0.6	107
136	On a construction of quadratic APN functions. , 2009, , .		27
137	Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications. IEEE Transactions on Information Theory, 2008, 54, 1262-1272.	1.5	69
138	Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. IEEE Transactions on Information Theory, 2008, 54, 2354-2357.	1.5	76
139	Two Classes of Quadratic APN Binomials Inequivalent to Power Functions. IEEE Transactions on Information Theory, 2008, 54, 4218-4229.	1.5	93
140	A Method of Construction of Balanced Functions with Optimum Algebraic Immunity. , 2008, , .		25
141	Lower bounds on the higher order nonlinearities of Boolean functions and their applications to the inverse function. , 2008, , .		4
142	On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and Their Generalizations. Lecture Notes in Computer Science, 2008, , 345-367.	1.0	18
143	An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. Lecture Notes in Computer Science, 2008, , 425-440.	1.0	142
144	On an improved correlation analysis of stream ciphers using multi-output Boolean functions and the related generalized notion of nonlinearity. Advances in Mathematics of Communications, 2008, 2, 201-221.	0.4	3

#	Article	IF	Citations
145	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
146	Nonlinearities of S-boxes. Finite Fields and Their Applications, 2007, 13, 121-135.	0.6	64
147	Authentication Schemes from Highly Nonlinear Functions. , 2006, , .		2
148	On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities. Lecture Notes in Computer Science, 2006, , 1-28.	1.0	44
149	Authentication Schemes from Highly Nonlinear Functions. Designs, Codes, and Cryptography, 2006, 40, 71-79.	1.0	17
150	Hyper-bent functions and cyclic codes. Journal of Combinatorial Theory - Series A, 2006, 113, 466-482.	0.5	49
151	Construction of bent functions via Niho power functions. Journal of Combinatorial Theory - Series A, 2006, 113, 779-798.	0.5	105
152	An infinite class of quadratic APN functions which are not equivalent to power mappings. , 2006, , .		29
153	On the Higher Order Nonlinearities of Algebraic Immune Functions. Lecture Notes in Computer Science, 2006, , 584-601.	1.0	32
154	Concatenating Indicators of Flats for Designing Cryptographic Functions. Designs, Codes, and Cryptography, 2005, 36, 189-202.	1.0	3
155	Piecewise Constructions of Bent and Almost Optimal Boolean Functions. Designs, Codes, and Cryptography, 2005, 37, 449-464.	1.0	20
156	On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks. Lecture Notes in Computer Science, 2005, , 49-62.	1.0	37
157	Vectorial Functions and Covering Sequences. Lecture Notes in Computer Science, 2004, , 215-248.	1.0	6
158	Highly nonlinear mappings. Journal of Complexity, 2004, 20, 205-244.	0.7	194
159	On the confusion and diffusion properties of Maioranaâ€“McFarland's and extended Maioranaâ€“McFarland's functions. Journal of Complexity, 2004, 20, 182-204.	0.7	37
160	On aÂNew Notion of Nonlinearity Relevant to Multi-output Pseudo-random Generators. Lecture Notes in Computer Science, 2004, , 291-305.	1.0	11
161	Algebraic Attacks and Decomposition of Boolean Functions. Lecture Notes in Computer Science, 2004, , 474-491.	1.0	270
162	Differential Power Analysis Model and Some Results. International Federation for Information Processing, 2004, , 127-142.	0.4	61

#	Article	IF	Citations
163	On the Secondary Constructions of Resilient and Bent Functions. , 2004, , 3-28.		48
164	On Plateaued Functions and Their Constructions. Lecture Notes in Computer Science, 2003, , 54-73.	1.0	51
165	On the Coset Weight Divisibility and Nonlinearity of Resilient and Correlation-Immune Functions. , 2002, , 131-144.		18
166	Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. Finite Fields and Their Applications, 2002, 8, 120-130.	0.6	53
167	An Upper Bound on the Number of m-Resilient Boolean Functions. Lecture Notes in Computer Science, 2002, , 484-496.	1.0	8
168	A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction. Lecture Notes in Computer Science, 2002, , 549-564.	1.0	49
169	On Generalized Bent and q-ary Perfect Nonlinear Functions. , 2001, , 81-94.		21
170	Bent, resilient functions and the numerical normal form. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 2001, , 87-96.	0.0	9
171	On the divisibility properties and nonlinearity of resilient functions. Comptes Rendus Mathematique, 2000, 331, 917-922.	0.5	7
172	Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. Lecture Notes in Computer Science, 2000, , 507-522.	1.0	60
173	A New Representation of Boolean Functions. Lecture Notes in Computer Science, 1999, , 94-103.	1.0	27
174	On Cryptographic Propagation Criteria for Boolean Functions. Information and Computation, 1999, 151, 32-56.	0.5	27
175	An Alternate Characterization of the Bentness of Binary Functions, with Uniqueness. Designs, Codes, and Cryptography, 1998, 14, 133-140.	1.0	21
176	Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. Designs, Codes, and Cryptography, 1998, 15, 125-156.	1.0	440
177	More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings. Lecture Notes in Computer Science, 1997, , 422-433.	1.0	29
178	A construction of bent functions. , 1996, , 47-58.		38
179	A Characterization of Binary Bent Functions. Journal of Combinatorial Theory - Series A, 1996, 76, 328-335.	0.5	48
180	Partially-bent functions. Designs, Codes, and Cryptography, 1993, 3, 135-145.	1.0	101

#	Article	IF	Citations
181	The automorphism groups of the Delsarte-Goethals codes. Designs, Codes, and Cryptography, 1993, 3, 237-249.	1.0	2
182	Two New Classes of Bent Functions. , 1993, , 77-101.		111
183	The Automorphism Groups of the Kerdock Codes. Journal of Information and Optimization Sciences, 1991, 12, 387-400.	0.2	4
184	A transformation on boolean functions, its consequences on some problems related to reed-muller codes. Lecture Notes in Computer Science, 1991, , 42-50.	1.0	15
185	A simple description of Kerdock codes. , 1988, , 202-208.		9
186	Best Information is Most Successful. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 49-79.	0.0	42
187	Boolean functions with restricted input and their robustness; application to the FLIP cipher. IACR Transactions on Symmetric Cryptology, 0, , 192-227.	0.0	29