

# Guang Gong

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/9607645/publications.pdf>

Version: 2024-02-01

177  
papers

3,853  
citations

186265

28  
h-index

223800

46  
g-index

179  
all docs

179  
docs citations

179  
times ranked

1629  
citing authors

#	ARTICLE	IF	CITATIONS
1	On ideal $t$ -tuple distribution of orthogonal functions in filtering de bruijn generators. Advances in Mathematics of Communications, 2022, 16, 597.	0.7	1
2	Polaris: Transparent Succinct Zero-Knowledge Arguments for R1CS with Efficient Verifier. Proceedings on Privacy Enhancing Technologies, 2022, 2022, 544-564.	2.8	1
3	New Constructions of Complementary Sequence Pairs Over $4^q$ -QAM. IEEE Transactions on Information Theory, 2022, 68, 2067-2082.	2.4	2
4	Correlation Power Analysis and Higher-Order Masking Implementation of WAGE. Lecture Notes in Computer Science, 2021, , 593-614.	1.3	3
5	New Construction of Complementary Sequence (or Array) Sets and Complete Complementary Codes. IEEE Transactions on Information Theory, 2021, 67, 4902-4928.	2.4	28
6	The Fourier spectral characterization for the correlation-immune functions over $\mathbb{F}_p$ . Cryptography and Communications, 2020, 12, 585-595.	1.4	1
7	Cycle Structures of a Class of Cascaded FSRs. IEEE Transactions on Information Theory, 2020, 66, 3766-3774.	2.4	1
8	A New Construction of QAM Golay Complementary Sequence Pair. , 2020, , .		0
9	Review of the EMC Aspects of Internet of Things. IEEE Transactions on Electromagnetic Compatibility, 2020, 62, 2604-2612.	2.2	15
10	Analysis and Efficient Implementations of a Class of Compositied de Bruijn Sequences. IEEE Transactions on Computers, 2020, 69, 1835-1848.	3.4	7
11	Lempel-Ziv Compression with Randomized Input-Output for Anti-compression Side-Channel Attacks Under HTTPS/TLS. Lecture Notes in Computer Science, 2020, , 117-136.	1.3	1
12	Error analysis of weak Poly-LWE instances. Cryptography and Communications, 2019, 11, 411-426.	1.4	1
13	A New Generalized Paraunitary Generator for Complementary Sets and Complete Complementary Codes of Size $2^m$ . IEEE Signal Processing Letters, 2019, 26, 4-8.	3.6	13
14	Secure simultaneous bit extraction from Koblitz curves. Designs, Codes, and Cryptography, 2019, 87, 1-13.	1.6	6
15	Mesh: A Supply Chain Solution with Locally Private Blockchain Transactions. Proceedings on Privacy Enhancing Technologies, 2019, 2019, 149-169.	2.8	9
16	Securing Internet-of-Things. Lecture Notes in Computer Science, 2019, , 3-16.	1.3	4
17	Notice of Retraction: Review of the EMC Aspects of Internet of Things. IEEE Transactions on Electromagnetic Compatibility, 2018, 60, 1152-1160.	2.2	7
18	Solomon W. Golomb—Mathematician, Engineer, and Pioneer. IEEE Transactions on Information Theory, 2018, 64, 2844-2857.	2.4	18

#	ARTICLE	IF	CITATIONS
19	Towards a Cryptographic Minimal Design: The sLiSCP Family of Permutations. IEEE Transactions on Computers, 2018, 67, 1341-1358.	3.4	7
20	Discrete Fourier Transform of Boolean Functions over the Complex Field and Its Applications. IEEE Transactions on Information Theory, 2018, 64, 3000-3009.	2.4	6
21	On ideal t-tuple distribution of filtering de Bruijn sequence generators. Cryptography and Communications, 2018, 10, 629-641.	1.4	2
22	A Direct Method to Construct Golay Complementary Sets Based on Boolean Functions. , 2018, , .		1
23	<scp>S</scp> L <scp>l</scp> SCP-light. Transactions on Embedded Computing Systems, 2018, 17, 1-26.	2.9	10
24	Rapid Hardware Design for Cryptographic Modules with Filtering Structures over Small Finite Fields. Lecture Notes in Computer Science, 2018, , 128-145.	1.3	2
25	Efficient Composed de Bruijn Sequence Generators. IEEE Transactions on Computers, 2017, 66, 1354-1368.	3.4	13
26	MILP-Based Cube Attack on the Reduced-Round WG-5 Lightweight Stream Cipher. Lecture Notes in Computer Science, 2017, , 333-351.	1.3	5
27	A new method to construct golay complementary set and near-complementary set by paraunitary matrices. , 2017, , .		6
28	A Novel Secure Transmission Scheme in MIMO Two-Way Relay Channels with Physical Layer Approach. Mobile Information Systems, 2017, 2017, 1-12.	0.6	1
29	Lelantos: A Blockchain-Based Anonymous Physical Delivery System. , 2017, , .		23
30	New almost perfect, odd perfect, and perfect sequences from difference balanced functions with $\langle i \rangle$ -form property. Advances in Mathematics of Communications, 2017, 11, 67-76.	0.7	3
31	More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$ . Designs, Codes, and Cryptography, 2016, 78, 391.	1.6	21
32	Two new message authentication codes based on APN functions and stream ciphers. Security and Communication Networks, 2016, 9, 1864-1871.	1.5	0
33	Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions. Cryptography and Communications, 2016, 8, 291-311.	1.4	6
34	Physical Layer Secure Information Exchange Protocol for MIMO Ad Hoc Networks against Passive Attacks. , 2016, , .		3
35	On algebraic immunity of trace inverse functions on finite fields of characteristic two. Journal of Systems Science and Complexity, 2016, 29, 272-288.	2.8	1
36	Quadratic zero-difference balanced functions, APN functions and strongly regular graphs. Designs, Codes, and Cryptography, 2016, 78, 629-654.	1.6	7

#	ARTICLE	IF	CITATIONS
37	Feedback Reconstruction and Implementations of Pseudorandom Number Generators from Compositd De Bruijn Sequences. IEEE Transactions on Computers, 2016, 65, 2725-2738.	3.4	16
38	Analysis and Validation of Active Eavesdropping Attacks in Passive FHSS RFID Systems. IEEE Transactions on Information Forensics and Security, 2016, 11, 1528-1541.	6.9	16
39	On $\Omega$ -cyclic-conjugated-perfect quaternary GDJ sequences. Advances in Mathematics of Communications, 2016, 10, 321-331.	0.7	0
40	On the existence of aperiodic complementary hexagonal lattice arrays. , 2016, , 341-362.		0
41	Conference key establishment protocol using a multivariate polynomial and its applications. Security and Communication Networks, 2015, 8, 1794-1800.	1.5	7
42	Integer arithmetic over ciphertext and homomorphic data aggregation. , 2015, , .		6
43	XOR Encryption Versus Phase Encryption, an In-Depth Analysis. IEEE Transactions on Electromagnetic Compatibility, 2015, 57, 903-911.	2.2	24
44	Sequences with good correlation property based on depth and interleaving techniques. Designs, Codes, and Cryptography, 2015, 77, 255-275.	1.6	1
45	$\{29, 11\}$ and $\{16\}$ and WG-Stream. IEEE Tran	3.4	7
46	The Simeck Family of Lightweight Block Ciphers. Lecture Notes in Computer Science, 2015, , 307-329.	1.3	142
47	WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices. EAI Endorsd Transactions on Security and Safety, 2015, 2, e4.	0.6	5
48	New binary sequences with good correlation based on high-order difference and interleaving techniques. , 2014, , .		0
49	Truly Random Number Generator Based on a Ring Oscillator Utilizing Last Passage Time. IEEE Transactions on Circuits and Systems II: Express Briefs, 2014, 61, 937-941.	3.0	41
50	Optimal parameters for the WG stream cipher family. Cryptography and Communications, 2014, 6, 117-135.	1.4	8
51	On the PMEPR of Binary Golay Sequences of Length $2^n$ . IEEE Transactions on Information Theory, 2014, 60, 2391-2398.	2.4	13
52	New Families of Optimal Frequency-Hopping Sequences of Composite Lengths. IEEE Transactions on Information Theory, 2014, 60, 3688-3697.	2.4	21
53	Novel last passage time based jitter model with application to low slew rate/high noise ring oscillator. Analog Integrated Circuits and Signal Processing, 2014, 78, 853-863.	1.4	4
54	A new efficient physical layer OFDM encryption scheme. , 2014, , .		22

#	ARTICLE	IF	CITATIONS
55	The Proof of Lin's Conjecture via the Decimation-Hadamard Transform. IEEE Transactions on Information Theory, 2014, 60, 5054-5064.	2.4	12
56	New Implementations of the WG Stream Cipher. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, 22, 1865-1878.	3.1	10
57	Fuzzy Authorization for Cloud Storage. IEEE Transactions on Cloud Computing, 2014, 2, 422-435.	4.4	24
58	Multidimensional meet-in-the-middle attack and its applications to KATAN32/48/64. Cryptography and Communications, 2014, 6, 313-333.	1.4	19
59	Generating Good Span n Sequences Using Orthogonal Functions in Nonlinear Feedback Shift Registers. , 2014, , 127-162.		4
60	New Polyphase Sequence Families With Low Correlation Derived From the Weil Bound of Exponential Sums. IEEE Transactions on Information Theory, 2013, 59, 3990-3998.	2.4	12
61	Framework for MIMO cross-layer secure communication based on STBC. Telecommunication Systems, 2013, 52, 2177-2185.	2.5	11
62	Large Zero Autocorrelation Zones of Golay Sequences and Their Applications. IEEE Transactions on Communications, 2013, 61, 3967-3979.	7.8	36
63	Resilience to distinguishing attacks on WG-7 cipher and their generalizations. Cryptography and Communications, 2013, 5, 277-289.	1.4	7
64	On selection of optimal parameters for the WG stream cipher family. , 2013, , .		5
65	Randomness properties of stream ciphers for wireless communications. , 2013, , .		5
66	On the Node Clone Detection in Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 2013, 21, 1799-1811.	3.8	16
67	Secure and Efficient LCMQ Entity Authentication Protocol. IEEE Transactions on Information Theory, 2013, 59, 4042-4054.	2.4	12
68	Cryptographically Strong de Bruijn Sequences with Large Periods. Lecture Notes in Computer Science, 2013, , 104-118.	1.3	19
69	Hardware implementations of the WG-5 cipher for passive RFID tags. , 2013, , .		10
70	Design space exploration of the lightweight stream cipher WG-8 for FPGAs and ASICs. , 2013, , .		10
71	Large zero correlation zone of Golay pairs and QAM Golay pairs. , 2013, , .		3
72	Filtering Nonlinear Feedback Shift Registers Using Welch-Gong Transformations for Securing RFID Applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2013, , 643-657.	0.3	2

#	ARTICLE	IF	CITATIONS
73	Even periodic and odd periodic complementary sequence pairs from generalized Boolean functions. <i>Advances in Mathematics of Communications</i> , 2013, 7, 113-125.	0.7	3
74	Correlation of binary sequence families derived from the multiplicative characters of finite fields. <i>Advances in Mathematics of Communications</i> , 2013, 7, 475-484.	0.7	0
75	Large zero odd periodic autocorrelation zone of Golay sequences and QAM Golay sequences. , 2012, , .		6
76	Large zero periodic autocorrelation zone of Golay sequences. , 2012, , .		2
77	Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers. , 2012, , .		168
78	Accelerating signature-based broadcast authentication for wireless sensor networks. <i>Ad Hoc Networks</i> , 2012, 10, 723-736.	5.5	37
79	A Three-Valued Walsh Transform From Decimations of Hellesteth-Gong Sequences. <i>IEEE Transactions on Information Theory</i> , 2012, 58, 1158-1162.	2.4	9
80	On the Dual of Certain Ternary Weakly Regular Bent Functions. <i>IEEE Transactions on Information Theory</i> , 2012, 58, 2237-2243.	2.4	24
81	BUPL: Securing Passive RFID Communication through Physical Layer Enhancements. <i>Lecture Notes in Computer Science</i> , 2012, , 127-146.	1.3	5
82	Odd Perfect Sequences and Sets of Spreading Sequences with Zero or Low Odd Periodic Correlation Zone. <i>Lecture Notes in Computer Science</i> , 2012, , 1-12.	1.3	11
83	New Three-Valued Walsh Transforms from Decimations of Hellesteth-Gong Sequences. <i>Lecture Notes in Computer Science</i> , 2012, , 327-337.	1.3	2
84	On the (in)security of two Joint Encryption and Error Correction schemes. <i>International Journal of Security and Networks</i> , 2011, 6, 191.	0.2	11
85	Trace Representation and Linear Complexity of Binary $s$ th Power Residue Sequences of Period $sp$ . <i>IEEE Transactions on Information Theory</i> , 2011, 57, 1530-1547.	2.4	20
86	New Sequences Design From Weil Representation With Low Two-Dimensional Correlation in Both Time and Phase Shifts. <i>IEEE Transactions on Information Theory</i> , 2011, 57, 4600-4611.	2.4	15
87	Fast Discrete Fourier Spectra Attacks on Stream Ciphers. <i>IEEE Transactions on Information Theory</i> , 2011, 57, 5555-5565.	2.4	25
88	Upper bound for algebraic immunity on a subclass of Maiorana McFarland class of bent functions. <i>Information Processing Letters</i> , 2011, 111, 247-249.	0.6	6
89	Computationally efficient mutual entity authentication in wireless sensor networks. <i>Ad Hoc Networks</i> , 2011, 9, 204-215.	5.5	8
90	A SURVEY OF KEY REVOCATION SCHEMES IN MOBILE AD HOC NETWORKS. , 2011, , 265-281.		0

#	ARTICLE	IF	CITATIONS
91	Remedying the Hummingbird Cryptographic Algorithm. , 2011, , .		2
92	PERIODS ON TWO KINDS OF NONLINEAR FEEDBACK SHIFT REGISTERS WITH TIME VARYING FEEDBACK FUNCTIONS. International Journal of Foundations of Computer Science, 2011, 22, 1317-1329.	1.1	33
93	A framework of physical layer technique assisted authentication for vehicular communication networks. Science China Information Sciences, 2010, 53, 1996-2004.	4.3	2
94	New Constructions of Binary Sequences With Optimal Autocorrelation Value/Magnitude. IEEE Transactions on Information Theory, 2010, 56, 1278-1286.	2.4	66
95	New Sets of Zero or Low Correlation Zone Sequences via Interleaving Techniques. IEEE Transactions on Information Theory, 2010, 56, 1702-1713.	2.4	33
96	New Construction of $M$ -ary Sequence Families With Low Correlation From the Structure of Sidelnikov Sequences. IEEE Transactions on Information Theory, 2010, 56, 4061-4070.	2.4	31
97	Multiplicative Characters, the Weil Bound, and Polyphase Sequence Families With Low Correlation. IEEE Transactions on Information Theory, 2010, 56, 6376-6387.	2.4	23
98	A note on the diagonalization of the discrete Fourier transform. Applied and Computational Harmonic Analysis, 2010, 28, 114-120.	2.2	3
99	Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices. Lecture Notes in Computer Science, 2010, , 3-18.	1.3	85
100	MIMO Cross-Layer Secure Communication Architecture Based on STBC. , 2010, , .		5
101	A Lightweight Stream Cipher WG-7 for RFID Encryption and Authentication. , 2010, , .		40
102	On the structure of $M$ -ary Sidelnikov sequences of period $p \leq 2m$ & #x2212; 1. , 2010, , .		0
103	A new class of ternary and quaternary sequences with two-level autocorrelation. , 2010, , .		2
104	Generalized constructions of polyphase sequence families using shift and addition of multiplicative character sequences. , 2010, , .		0
105	A framework toward a self-organizing and self-healing certificate authority group in a Content Addressable Network. , 2010, , .		2
106	Near-Complementary Sequences of Various Lengths and Low PMEPR for Multicarrier Communications. , 2009, , .		0
107	A cross-layer approach to enhance the security of wireless networks based on MIMO. , 2009, , .		2
108	A Novel Framework for Message Authentication in Vehicular Communication Networks. , 2009, , .		25

#	ARTICLE	IF	CITATIONS
109	Algebraic Immunity of S-Boxes Based on Power Mappings: Analysis and Construction. IEEE Transactions on Information Theory, 2009, 55, 4263-4273.	2.4	16
110	New Results on Periodic Sequences With Large $\delta$ -Error Linear Complexity. IEEE Transactions on Information Theory, 2009, 55, 4687-4694.	2.4	12
111	A trace representation of binary Jacobi sequences. Discrete Mathematics, 2009, 309, 1517-1527.	0.7	20
112	Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks. , 2009, , .		9
113	New sequence families with zero or low correlation zone via interleaving techniques. , 2009, , .		2
114	Build-in wiretap channel I with feedback and LDPC codes. Journal of Communications and Networks, 2009, 11, 538-543.	2.6	14
115	Lightweight implementation of Hummingbird cryptographic algorithm on 4-bit microcontrollers. , 2009, , .		13
116	Time-Memory-Data Trade-Off Attack on Stream Ciphers Based on Maiorana-McFarland Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 11-21.	0.3	4
117	A generalized construction of OFDM $M$ -QAM sequences with low peak-to-average power ratio. Advances in Mathematics of Communications, 2009, 3, 421-428.	0.7	5
118	Highly nonlinear balanced S-boxes with improved bound on unrestricted and generalized nonlinearity. Applicable Algebra in Engineering, Communications and Computing, 2008, 19, 323-338.	0.5	2
119	WG: A family of stream ciphers with designed randomness properties. Information Sciences, 2008, 178, 1903-1916.	6.9	46
120	A New Class of Sequences With Zero or Low Correlation Zone Based on Interleaving Technique. IEEE Transactions on Information Theory, 2008, 54, 4267-4273.	2.4	93
121	Hyperbent Functions, Kloosterman Sums, and Dickson Polynomials. IEEE Transactions on Information Theory, 2008, 54, 4230-4238.	2.4	76
122	New Binary Sequences With Optimal Autocorrelation Magnitude. IEEE Transactions on Information Theory, 2008, 54, 4771-4779.	2.4	33
123	Key revocation based on Dirichlet multinomial model for mobile ad hoc networks. , 2008, , .		1
124	Hyperbent functions, Kloosterman sums and Dickson polynomials. , 2008, , .		13
125	Constructions of Multiple Shift-Distinct Signal Sets with Low Correlation. , 2007, , .		14
126	Actions of the Unitary Group on Irreducible/Primitive Polynomials and Their Applications to Randomness of Sequences. , 2007, , .		1

#	ARTICLE	IF	CITATIONS
127	Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks. International Journal of Security and Networks, 2007, 2, 239.	0.2	10
128	Correlation of Multiple Bent Function Signal Sets. , 2007, , .		3
129	A Note on Low-Correlation Zone Signal Sets. IEEE Transactions on Information Theory, 2007, 53, 2575-2581.	2.4	37
130	The Status of Costas Arrays. IEEE Transactions on Information Theory, 2007, 53, 4260-4265.	2.4	33
131	Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes. , 2007, , 313-337.		13
132	Crosscorrelation of q-ary Power Residue Sequences of Period p. , 2006, , .		11
133	Integrated DH-like Key Exchange Protocols from LUC, GH and XTR. , 2006, , .		1
134	A Note on Low Correlation Zone Signal Sets. , 2006, , .		1
135	Two-tuple balance of non-binary sequences with ideal two-level autocorrelation. Discrete Applied Mathematics, 2006, 154, 2590-2598.	0.9	26
136	A New Characterization of Semi-bent and Bent Functions on Finite Fields*. Designs, Codes, and Cryptography, 2006, 38, 279-295.	1.6	71
137	A new binary sequence family with low correlation and large size. IEEE Transactions on Information Theory, 2006, 52, 1624-1636.	2.4	39
138	Constructions of quadratic bent functions in polynomial forms. IEEE Transactions on Information Theory, 2006, 52, 3291-3299.	2.4	57
139	Interleaved Construction of Binary Sequences with Optimal Autocorrelation Magnitude. , 2006, , .		1
140	The editing generator and its cryptanalysis. International Journal of Wireless and Mobile Computing, 2005, 1, 46.	0.2	1
141	Maximum correlation of binary signals over fading channels. , 2005, , .		1
142	Asymptotic Behavior of Normalized Linear Complexity of Ultimately Nonperiodic Binary Sequences. IEEE Transactions on Information Theory, 2004, 50, 2911-2915.	2.4	12
143	Additive Autocorrelation of Resilient Boolean Functions. Lecture Notes in Computer Science, 2004, , 275-290.	1.3	13
144	Trace representation of binary e-th residue sequences of period p. , 2003, , .		0

#	ARTICLE	IF	CITATIONS
145	Trace representation of binary jacobi sequences. , 2003, , .		0
146	New Constructions for Resilient and Highly Nonlinear Boolean Functions. Lecture Notes in Computer Science, 2003, , 498-509.	1.3	8
147	Cryptographic properties of the Welch-Gong transformation sequence generators. IEEE Transactions on Information Theory, 2002, 48, 2837-2846.	2.4	52
148	New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case. IEEE Transactions on Information Theory, 2002, 48, 2847-2867.	2.4	129
149	New nonbinary sequences with ideal two-level autocorrelation. IEEE Transactions on Information Theory, 2002, 48, 2868-2872.	2.4	61
150	On interleaved sequences over finite fields. Discrete Mathematics, 2002, 252, 161-178.	0.7	6
151	Hyper-bent Functions. Lecture Notes in Computer Science, 2001, , 406-419.	1.3	49
152	New Families of Ideal 2-Level Autocorrelation Ternary Sequences From Second Order DHT. Electronic Notes in Discrete Mathematics, 2001, 6, 375-384.	0.4	10
153	A conjecture on binary sequences with the "trinomial property". IEEE Transactions on Information Theory, 2001, 47, 426-427.	2.4	0
154	Boolean Functions with Large Distance to All Bijective Monomials: N Odd Case. Lecture Notes in Computer Science, 2001, , 49-59.	1.3	4
155	Cyclic inequivalence of cascaded GMW-sequences. Discrete Mathematics, 2000, 219, 279-285.	0.7	2
156	Enumeration and criteria for cyclically shift-distinct GMW sequences. IEEE Transactions on Information Theory, 2000, 46, 474-484.	2.4	3
157	On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code. IEEE Transactions on Information Theory, 2000, 46, 680-687.	2.4	21
158	Notes on q-ary interleaved sequences. Science Bulletin, 2000, 45, 502-507.	1.7	1
159	Elliptic Curve Pseudorandom Sequence Generators. Lecture Notes in Computer Science, 2000, , 34-48.	1.3	35
160	Generating all linear orthomorphisms without repetition. Discrete Mathematics, 1999, 205, 47-55.	0.7	11
161	Binary sequences with two-level autocorrelation. IEEE Transactions on Information Theory, 1999, 45, 692-693.	2.4	13
162	Periodic binary sequences with the "trinomial property". IEEE Transactions on Information Theory, 1999, 45, 1276-1279.	2.4	15

#	ARTICLE	IF	CITATIONS
163	Hadamard transforms of three-term sequences. IEEE Transactions on Information Theory, 1999, 45, 2059-2060.	2.4	6
164	Transform domain analysis of DES. IEEE Transactions on Information Theory, 1999, 45, 2065-2073.	2.4	43
165	Public-key cryptosystems based on cubic finite field extensions. IEEE Transactions on Information Theory, 1999, 45, 2601-2605.	2.4	81
166	Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation. IEEE Transactions on Information Theory, 1998, 44, 814-817.	2.4	74
167	A new class of nonlinear PN sequences over $GF(q^n)$ . IEEE Transactions on Information Theory, 1997, 43, 1007-1012.	2.4	2
168	Q-ary cascaded GMW sequences. IEEE Transactions on Information Theory, 1996, 42, 263-267.	2.4	36
169	Theory and applications of q-ary interleaved sequences. IEEE Transactions on Information Theory, 1995, 41, 400-411.	2.4	174
170	Synthesis and uniqueness of m-sequences over $GF(q^n)$ as n-phase sequences over $GF(q)$ . IEEE Transactions on Communications, 1994, 42, 2501-2505.	7.8	8
171	New nonbinary sequences with ideal two-level autocorrelation function. , 0, , .		10
172	Efficient key agreement and signature schemes using compact representations in $GF(p^{10})$ . , 0, , .		3
173	Improved cascade stream ciphers using feedback. , 0, , .		0
174	Short Paper: Limitations of Key Escrow in Identity-Based Schemes in Ad Hoc Networks. , 0, , .		1
175	Quadratic Bent Functions of Polynomial Forms and their Applications to Bent Sequences. , 0, , .		1
176	An Efficient Stream Cipher WG-16 and its Application for Securing 4G-LTE Networks. Applied Mechanics and Materials, 0, 490-491, 1436-1450.	0.2	2
177	WAGE: An Authenticated Encryption with a Twist. IACR Transactions on Symmetric Cryptology, 0, , 132-159.	0.0	17