Franco Chiaraluce

List of Publications by Year
in descending order

133 papers	1,435 citations	394286 19 h-index	454834 30 g-index
133 all docs	133 docs citations	133 times ranked	753 citing authors

#	Article	IF	Citations
1	Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis. IEEE Transactions on Information Forensics and Security, 2012, 7, 883-894.	4.5	110
2	A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes. Lecture Notes in Computer Science, 2008, , 246-262.	1.0	84
3	Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes. , 2007, , .		76
4	Enhanced Public Key Security for the McEliece Cryptosystem. Journal of Cryptology, 2016, 29, 1-27.	2.1	60
5	Non-systematic codes for physical layer security. , 2010, , .		54
6	Security and complexity of the McEliece cryptosystem based on quasi€cyclic low€density parity€check codes. IET Information Security, 2013, 7, 212-220.	1.1	51
7	Channel Coding for Future Space Missions: New Requirements and Trends. Proceedings of the IEEE, 2007, 95, 2157-2170.	16.4	36
8	Chaos-Based Radars for Automotive Applications: Theoretical Issues and Numerical Simulation. IEEE Transactions on Vehicular Technology, 2008, 57, 3858-3863.	3.9	33
9	On a Family of Circulant Matrices for Quasi-Cyclic Low-Density Generator Matrix Codes. IEEE Transactions on Information Theory, 2011, 57, 6052-6067.	1.5	33
10	Secrecy Transmission on Parallel Channels: Theoretical Limits and Performance of Practical Codes. IEEE Transactions on Information Forensics and Security, 2014, 9, 1765-1779.	4.5	33
11	Design and Analysis of Time-Invariant SC-LDPC Convolutional Codes With Small Constraint Length. IEEE Transactions on Communications, 2018, 66, 918-931.	4.9	33
12	LEDAkem: A Post-quantum Key Encapsulation Mechanism Based on QC-LDPC Codes. Lecture Notes in Computer Science, 2018, , 3-24.	1.0	31
13	Finite-Precision Analysis of Demappers and Decoders for LDPC-Coded M-QAM Systems. IEEE Transactions on Broadcasting, 2009, 55, 239-250.	2.5	27
14	A Finite Regime Analysis of Information Set Decoding Algorithms. Algorithms, 2019, 12, 209.	1.2	27
15	Non-Invasive UWB Sensing of Astronautsâ€™ Breathing Activity. Sensors, 2015, 15, 565-591.	2.1	26
16	LDPC codes based on serially concatenated multiple parity-check codes. IEEE Communications Letters, 2009, 13, 142-144.	2.5	25
17	Efficient Search of Compact QC-LDPC and SC-LDPC Convolutional Codes With Large Girth. IEEE Communications Letters, 2018, 22, 1156-1159.	2.5	25
18	A comparison between APSK and QAM in wireless tactical scenarios for land mobile systems. Eurasip Journal on Wireless Communications and Networking, 2012, 2012, .	1.5	23

#	Article	IF	Citations
19	Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel. , 2015, , .		23
20	On the use of ordered statistics decoders for low-density parity-check codes in space telecommand links. Eurasip Journal on Wireless Communications and Networking, 2016, 2016, .	1.5	23
21	A Hybrid Decoding Scheme for Short Non-Binary LDPC Codes. IEEE Communications Letters, 2014, 18, 2093-2096.	2.5	21
22	Analysis of the Error Correction Capability of LDPC and MDPC Codes Under Parallel Bit-Flipping Decoding and Application to Cryptography. IEEE Transactions on Communications, 2020, 68, 4648-4660.	4.9	19
23	Optimization of the parity-check matrix density in QC-LDPC code-based McEliece cryptosystems. , 2013, , .		18
24	Using LDGM Codes and Sparse Syndromes to Achieve Digital Signatures. Lecture Notes in Computer Science, 2013, , 1-15.	1.0	18
25	Increasing Physical Layer Security through Scrambled Codes and ARQ. , 2011, , .		17
26	On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. , 2006, , .		16
27	A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks. IEEE Wireless Communications Letters, 2013, 2, 183-186.	3.2	16
28	Array Convolutional Low-Density Parity-Check Codes. IEEE Communications Letters, 2014, 18, 336-339.	2.5	16
29	Interleaved Product LDPC Codes. IEEE Transactions on Communications, 2012, 60, 895-901.	4.9	15
30	Compact QC-LDPC Block and SC-LDPC Convolutional Codes for Low-Latency Communications. , 2018, , .		15
31	Efficiency of the gossip algorithm for wireless sensor networks. , 2007, , .		13
32	Progressive Differences Convolutional Low-Density Parity-Check Codes. IEEE Communications Letters, 2012, 16, 1848-1851.	2.5	13
33	Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes. , 2013, , .		12
34	Analysis of Reaction and Timing Attacks Against Cryptosystems Based on Sparse Parity-Check Codes. Lecture Notes in Computer Science, 2019, , 115-136.	1.0	12
35	On the Autocorrelation Properties of Truncated Maximum-Length Sequences and Their Effect on the Power Spectrum. IEEE Transactions on Signal Processing, 2010, 58, 6284-6297.	3.2	11
36	Analysis and performance evaluation of new coding options for space telecommand links â€•Part I: AWGN channels. International Journal of Satellite Communications and Networking, 2015, 33, 509-525.	1.2	11

#	Article	IF	Citations
37	Recent progress in fibre optics. Progress in Quantum Electronics, 1994, 18, 39-95.	3.5	9
38	Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors. , 2016, , .		9
39	Hindering Reaction Attacks by Using Monomial Codes in the McEliece Cryptosystem. , 2018, , .		9
40	LEDAcrypt: QC-LDPC Code-Based Cryptosystems with Bounded Decryption Failure Rate. Lecture Notes in Computer Science, 2019, , 11-43.	1.0	9
41	A Data-Driven Approach to Cyber Risk Assessment. Security and Communication Networks, 2019, 2019, 1-8.	1.0	9
42	A Simple Scheme for Belief Propagation Decoding of BCH and RS Codes in Multimedia Transmissions. International Journal of Digital Multimedia Broadcasting, 2008, 2008, 1-12.	0.4	8
43	Analysis and simulation of algorithms for vital signs detection using UWB radars. , 2011, , .		8
44	On fuzzy syndrome hashing with LDPC coding. , 2011, , .		8
45	Body movement compensation in UWB radars for respiration monitoring. , 2012, , .		8
46	Cryptanalysis of a One-Time Code-Based Digital Signature Scheme. , 2019, , .		8
47	Code-based physical layer secret key generation in passive optical networks. Ad Hoc Networks, 2019, 89, 1-8.	3.4	8
48	Low-power secret-key agreement over OFDM. , 2013, , .		7
49	Analysis and performance evaluation of new coding options for space telecommand links â€" part II: jamming channels. International Journal of Satellite Communications and Networking, 2015, 33, 527-542.	1.2	7
50	Interleaver Design for Short Concatenated Codes. IEEE Communications Letters, 2018, 22, 1762-1765.	2.5	7
51	Hard-Decision Iterative Decoding of LDPC Codes with Bounded Error Rate. , 2019, , .		7
52	Coded transmissions for space links affected by solar scintillation: Baseband analysis. International Journal of Satellite Communications and Networking, 2019, 37, 571-587.	1.2	7
53	Efficient Hardware Implementation of the LEDAcrypt Decoder. IEEE Access, 2021, 9, 66223-66240.	2.6	7
54	Impact of truncation on the statistical properties of LFSR sequences. , 2009, , .		6

#	Article	IF	Citations
55	Performance of Gossip Algorithms in Wireless Sensor Networks. Lecture Notes in Electrical Engineering, 2011, , 3-16.	0.3	6
56	A Class of Punctured Simplex Codes Which Are Proper for Error Detection. IEEE Transactions on Information Theory, 2012, 58, 3861-3880.	1.5	6
57	On the applicability of the most reliable basis algorithm for LDPC decoding in telecommand links. , 2015, , .		6
58	On the error detection capability of combined LDPC and CRC codes for space telecommand transmissions. , 2016, , .		6
59	Physical layer security over fading wiretap channels through classic coded transmissions with finite block length and discrete modulation. Physical Communication, 2019, 37, 100829.	1.2	6
60	Girth Properties of Time-Varying SC-LDPC Convolutional Codes. , 2019, , .		6
61	Using Non-Binary LDPC and MDPC Codes in the McEliece Cryptosystem. , 2019, , .		6
62	Efficiency Tests Results and New Perspectives for Secure Telecommand Authentication in Space Missions: Case-Study of the European Space Agency. ETRI Journal, 2005, 27, 394-404.	1.2	6
63	Enhancements of DQDB protocol with ECBWB mechanism for fair access and multi-priority traffic management. Computer Communications, 1993, 16, 511-517.	3.1	5
64	Variable Rate LDPC Codes for Wireless Applications. , 2006, , .		5
65	A Class of Low-Density Parity-Check Product Codes. , 2009, , .		5
66	Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels. Eurasip Journal on Wireless Communications and Networking, 2015, 2015, .	1.5	5
67	Improving deep space telecommunications during solar superior conjunctions. , 2017, , .		5
68	Efficient Search and Elimination of Harmful Objects for the Optimization of QC-SC-LDPC Codes. , 2019, , .		5
69	Security of generalised Reedâ€"Solomon codeâ€based cryptosystems. IET Information Security, 2019, 13, 404-410.	1.1	5
70	End-to-End Simulations of Coded Transmissions in Space Links Affected by Solar Scintillation. IEEE Transactions on Aerospace and Electronic Systems, 2020, 56, 3259-3275.	2.6	5
71	A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems. , 2020, , .		5
72	Turbo Code Applications on Telemetry and Deep Space Communications. , 2005, , 321-344.		5

#	ARTICLE	IF	CITATIONS
73	MAGIC: A Method for Assessing Cyber Incidents Occurrence. IEEE Access, 2022, 10, 73458-73473.	2.6	5
74	Design techniques of two-layer architectures for WDM optical networks. International Journal of Communication Systems, 2001, 14, 171-188.	1.6	4
75	Simple Statistical Analysis of the Impact of Some Nonidealities in Downstream VDSL with Linear Precoding. Eurasip Journal on Advances in Signal Processing, 2010, 2010, .	1.0	4
76	Error correcting codes in telecommand and telemetry for European Space Agency missions: An overview and new perspectives. , 2014, , .		4
77	On the error probability of short concatenated polar and cyclic codes with interleaving. , 2017, , .		4
78	Girth Analysis and Design of Periodically Time-Varying SC-LDPC Codes. IEEE Transactions on Information Theory, 2021, 67, 2217-2235.	1.5	4
79	Performance Bounds forÂQC-MDPC Codes Decoders. Lecture Notes in Computer Science, 2022, , 95-122.	1.0	4
80	Azimuthal refractive index modulation for enhancing birefringence of elliptical single-mode fibres. Optics Communications, 1990, 78, 230-236.	1.0	3
81	Iterative soft-decision decoding of binary cyclic codes based on spread parity-check matrices. , 2007, , .		3
82	Comparison of Averaging Algorithms for Wireless Sensor Networks. , 2008, , .		3
83	Irregular M-SC-MPC codes for wireless applications. , 2010, , .		3
84	Performance of APSK modulation in wireless tactical scenarios for land mobile systems. , 2011, , .		3
85	Analysis of the Correlation Coefficient Between Component Noise Squared Norms for OFDM Systems. IEEE Signal Processing Letters, 2011, 18, 311-314.	2.1	3
86	Security gap assessment for the fast fading wiretap channel. , 2013, , .		3
87	Practical LDPC coded modulation schemes for the fading broadcast channel with confidential messages. , 2014, , .		3
88	LDPC coded transmissions over the Gaussian broadcast channel with confidential messages. , 2014, , .		3
89	Time-invariant spatially coupled low-density parity-check codes with small constraint length. , 2016, , .		3
90	On the security of transmissions over fading wiretap channels in realistic conditions. , 2017, , .		3

#	Article	IF	Citations
91	Security in heterogeneous distributed storage systems: A practically achievable information-theoretic approach. , 2017, , .		3
92	Theoretical Analysis and Implementation of Effective Receivers for Telecommand Space Links. , 2019, , .		3
93	A Probabilistic Small Model Theorem to Assess Confidentiality of Dispersed Cloud Storage. Lecture Notes in Computer Science, 2017, , 123-139.	1.0	3
94	Single-mode optical fibers with geometrical birefringence: Analysis of the propagation by means of finite element method. European Transactions on Telecommunications, 1991, 2, 335-342.	1.2	2
95	<title>Multicast routing in BMSNs through greedy, weighted greedy, and Dijkstra algorithms: a comparative analysis</title>. , 1998, , .		2
96	Symbol synchronization properties of CCSDS turbo codes. International Journal of Satellite Communications and Networking, 2002, 20, 379-390.	0.6	2
97	Design and comparison of turbo codes under frame-length and code-rate constraints. International Journal of Satellite Communications and Networking, 2006, 24, 241-259.	1.2	2
98	A Proposal of Automotive Anticollision Radars Based on Spread Spectrum Techniques. , 2007, , .		2
99	Exact and Approximate Expressions for the Probability of Undetected Errors of Varshamov-Tenengol'ts Codes. IEEE Transactions on Information Theory, 2008, 54, 5019-5029.	1.5	2
100	Some Remarks on the Problem of Spurious Frequencies in High Data Rate Space Missions. , 2009, , .		2
101	Security gap performance of some LDPC code constructions. , 2013, , .		2
102	A tight estimation of the security gap over the fast fading wiretap channel. , 2013, , .		2
103	A practical viewpoint on the performance of LDPC codes over the fast Rayleigh fading wire-tap channel. , 2013, , .		2
104	Sparse generator matrices for some families of Quasi-Cyclic Low-Density Parity-Check codes. , 2014, , .		2
105	On Non-Linear Codes Correcting Errors of Limited Size. , 2017, , .		2
106	Assessing and Countering Reaction Attacks Against Post-Quantum Public-Key Cryptosystems Based on QC-LDPC Codes. Lecture Notes in Computer Science, 2018, , 323-343.	1.0	2
107	Analysis of the Block Error Probability of Concatenated Polar Code Ensembles. IEEE Transactions on Communications, 2019, 67, 5953-5962.	4.9	2
108	Effect of randomizers on the power spectrum excess of space telemetry signals. International Journal of Satellite Communications and Networking, 2022, 40, 67-82.	1.2	2

#	Article	IF	Citations
109	Performance Analysis of Transmission over AWGN Wiretap Channels with Practical Codes. Lecture Notes in Electrical Engineering, 2016, , 53-68.	0.3	2
110	Performance Evaluation of Some Distributed Averaging Algorithms for Sensor Networks. International Journal of Distributed Sensor Networks, 2011, 7, 428290.	1.3	2
111	Performance analysis of trellis coded biorthogonal sequences in a variable rate system. European Transactions on Telecommunications, 1992, 3, 231-235.	1.2	1
112	Some analytical tools for the global performance evaluation of packet switching networks based on virtual paths. International Journal of Communication Systems, 1995, 8, 275-286.	1.6	1
113	PPM transmission over a photon counting channel: Comparison among various transmission formats. European Transactions on Telecommunications, 1996, 7, 359-376.	1.2	1
114	PROPOSAL OF A PACKET SWITCH BASED ON PURELY RANDOM ROUTING. International Journal of Communication Systems, 1996, 9, 145-150.	1.6	1
115	A class of invertible circulant matrices for QC-LDPC codes. , 2008, , .		1
116	Easily encodable LDPC codes based on polynomial codes. , 2008, , .		1
117	Telecommand Authentication in Space Missions: Cryptanalysis and Future Trends. IEEE Transactions on Aerospace and Electronic Systems, 2009, 45, 752-761.	2.6	1
118	On the Effect of Estimation and Quantization Errors in Downstream VDSL Systems. , 2010, , .		1
119	LDPC coded modulation schemes with largely unequal error protection. , 2015, , .		1
120	Semantic Security with Practical Transmission Schemes over Fading Wiretap Channels. Entropy, 2017, 19, 491.	1.1	1
121	Efficiency of Unicast and Broadcast Gossip Algorithms for Wireless Sensor Networks. Journal of Communications Software and Systems, 2017, 4, 105.	0.6	1
122	Optimal Share Factors in the Push-Sum Algorithm for Ring and Random Geometric Graph Sensor Networks. Journal of Communications Software and Systems, 2017, 5, 9.	0.6	1
123	A trusted cryptocurrency scheme for secure and verifiable digital transactions. First Monday, 0, , .	0.6	1
124	Analysis of In-Place Randomized Bit-Flipping Decoders for the Design of LDPC and MDPC Code-Based Cryptosystems. Communications in Computer and Information Science, 2021, , 151-174.	0.4	1
125	Next generation earth-to-space telecommand coding and synchronization: ground system design, optimization and software implementation. Eurasip Journal on Wireless Communications and Networking, 2021, 2021, .	1.5	1
126	Proposal and performance evaluation of a packet over VDSL protocol for increasing throughput in the transmission of IP packets. International Journal of Communication Systems, 2004, 17, 363-374.	1.6	0

#	Article	IF	Citations
127	Share factors optimization in the Push-Sum algorithm for sensor networks. , 2008, , .		0
128	Performance and complexity of &#x03C8;-unitary QC-LDGM codes. , 2009, , .		0
129	New LDPC Codes Based on Serial Concatenation. , 2009, , .		0
130	Achieving semantic security without keys through coding and all-or-nothing transforms over wireless channels. , 2016, , .		0
131	Off-line Correlator for Antenna Array Over Long Baselines. , 2019, , .		0
132	Complexity of statistical attacks on QCâ€‘LDPC codeâ€‘based cryptosystems. IET Information Security, 2020, 14, 304-312.	1.1	0
133	Telecommunications in the ICT Age: From Research to Applications. , 2019, , 53-71.		0