Amr M Youssef

List of Publications by Year in descending order

110 papers	2,561 citations	430874 18 h-index	223800 46 g-index
110 all docs	110 docs citations	110 times ranked	2562 citing authors

#	Article	IF	Citations
1	Confidentiality attacks against encrypted control systems. Cyber-Physical Systems, 2023, 9, 224-243.	2.0	3
2	Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management. IEEE Transactions on Industrial Informatics, 2022, 18, 1641-1653.	11.3	9
3	A Key-Agreement Scheme for Cyberâ€“Physical Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52, 5368-5373.	9.3	2
4	Et tu, Brute? Privacy Analysis of Government Websites and Mobile Apps. , 2022, , .		8
5	Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays. IEEE Transactions on Smart Grid, 2022, 13, 4787-4800.	9.0	12
6	Encrypted Cloud-Based Set-Theoretic Model Predictive Control. , 2022, 6, 3032-3037.		2
7	Edge Computing and Multiple-Association in Ultra-Dense Networks: Performance Analysis. IEEE Transactions on Communications, 2022, 70, 5098-5112.	7.8	9
8	A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays. IEEE Transactions on Power Delivery, 2021, 36, 2274-2286.	4.3	20
9	Threat Intelligence Generation Using Network Telescope Data for Industrial Control Systems. IEEE Transactions on Information Forensics and Security, 2021, 16, 3355-3370.	6.9	8
10	Covert Channels in Cyber-Physical Systems. , 2021, , .		1
11	Ergodic Secrecy Rate Analysis of Ultra-Dense Networks with Multiple Antennas. , 2021, , .		1
12	Multiple-Association Supporting HTC/MTC in Limited-Backhaul Capacity Ultra-Dense Networks. IEEE Transactions on Communications, 2021, 69, 4113-4127.	7.8	12
13	Covert channels in stochastic cyberâ€physical systems. IET Cyber-Physical Systems: Theory and Applications, 2021, 6, 228-237.	3.3	3
14	Covert Channels in Cyber-Physical Systems. , 2021, 5, 1273-1278.		11
15	Cyber Security of Market-Based Congestion Management Methods in Power Distribution Systems. IEEE Transactions on Industrial Informatics, 2021, 17, 8142-8153.	11.3	5
16	Parental Controls: Safer Internet Solutions or New Pitfalls?. IEEE Security and Privacy, 2021, , 2-12.	1.2	3
17	Efficient Inter-Cloud Authentication and Micropayment Protocol for IoT Edge Computing. IEEE Transactions on Network and Service Management, 2021, 18, 4420-4433.	4.9	6
18	On Securing Cloud-Hosted Cyber-Physical Systems Using Trusted Execution Environments. , 2021, , .		3

#	Article	IF	Citations
19	Lightweight Authentication and Key Agreement Protocol for Edge Computing Applications. , 2021, , .		1
20	LSTM-based approach to detect cyber attacks on market-based congestion management methods. , 2021, , .		0
21	An Intrusion Detection Method for Line Current Differential Relays. IEEE Transactions on Information Forensics and Security, 2020, 15, 329-344.	6.9	26
22	Uplink Coverage and Capacity Analysis of mMTC in Ultra-Dense Networks. IEEE Transactions on Vehicular Technology, 2020, 69, 746-759.	6.3	27
23	Set-Theoretic Control for Active Detection of Replay Attacks with Applications to Smart Grid. , 2020, , .		5
24	Cyberâ€“physical attacks on power distribution systems. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 218-225.	3.3	21
25	NOMA-Assisted Machine-Type Communications in UDN: State-of-the-Art and Challenges. IEEE Communications Surveys and Tutorials, 2020, 22, 1276-1304.	39.4	85
26	Lightweight Broadcast Authentication Protocol for Edge-Based Applications. IEEE Internet of Things Journal, 2020, 7, 11766-11777.	8.7	27
27	Uplink Performance of NOMA-Based Combined HTC and MTC in Ultradense Networks. IEEE Internet of Things Journal, 2020, 7, 7319-7333.	8.7	20
28	Wyner wiretapâ€like encoding scheme for cyberâ€physical systems. IET Cyber-Physical Systems: Theory and Applications, 2020, 5, 359-365.	3.3	3
29	A DoS-resilient Set-Theoretic Controller for Smart Grid Applications. , 2020, , .		2
30	Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions. , 2020, , .		7
31	A Hybrid NOMA/OMA Scheme for MTC in Ultra-Dense Networks. , 2020, , .		9
32	The Sorry State of TLS Security in Enterprise Interception Appliances. Digital Threats Research and Practice, 2020, 1, 1-26.	2.4	8
33	A Lightweight Authentication and Inter-Cloud Payment Protocol for Edge Computing. , 2020, , .		6
34	Capacity Analysis of Downlink NOMA-Based Coexistent HTC/MTC in UDN. , 2019, , .		15
35	Detecting, Fingerprinting and Tracking Reconnaissance Campaigns Targeting Industrial Control Systems. Lecture Notes in Computer Science, 2019, , 89-108.	1.3	5
36	Cyber Attacks On Distributed Congestion Management Methods. , 2019, , .		3

#	Article	IF	Citations
37	Impact of Electric Vehicles Botnets on the Power Grid. , 2019, , .		15
38	Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management1. , 2019, , .		5
39	Playing With Danger: A Taxonomy and Evaluation of Threats to Smart Toys. IEEE Internet of Things Journal, 2019, 6, 2986-3002.	8.7	26
40	Joint Detection and Mitigation of False Data Injection Attacks in AGC Systems. IEEE Transactions on Smart Grid, 2019, 10, 4985-4995.	9.0	89
41	An Efficient Micropayment Channel on Ethereum. Lecture Notes in Computer Science, 2019, , 211-218.	1.3	10
42	Attack Detection and Identification for Automatic Generation Control Systems. IEEE Transactions on Power Systems, 2018, 33, 4760-4774.	6.5	131
43	Attack Detection for Load Frequency Control Systems Using Stochastic Unknown Input Estimators. IEEE Transactions on Information Forensics and Security, 2018, 13, 2575-2590.	6.9	63
44	OpenStack-Based Evaluation Framework for Smart Grid Cyber Security. , 2018, , .		18
45	Improved Meet-in-the-Middle Attacks on Reduced Round Kuznyechik. Lecture Notes in Computer Science, 2018, , 26-38.	1.3	0
46	Detection of false data injection attacks in smart grids using Recurrent Neural Networks. , 2018, , .		63
47	Impossible Differential Attack on Reduced Round SPARX-128/256. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 731-733.	0.3	0
48	Related-Key Differential Attack on Round-Reduced Bel-T-256. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 859-862.	0.3	2
49	Performance Analysis of Multiple Association in Ultra-Dense Networks. IEEE Transactions on Communications, 2017, 65, 3818-3831.	7.8	70
50	Fault analysis on Kalyna. Information Security Journal, 2017, 26, 249-265.	1.9	2
51	Physical Layer Security in Ultra-Dense Networks. IEEE Wireless Communications Letters, 2017, 6, 690-693.	5.0	43
52	Security, Privacy, and Safety Aspects of Civilian Drones. ACM Transactions on Cyber-Physical Systems, 2017, 1, 1-25.	2.5	268
53	Downlink coverage and average cell load of M2M and H2H in ultra-dense networks. , 2017, , .		10
54	A power analysis resistant FPGA implementation of NTRUEncrypt. , 2017, , .		0

#	Article	IF	Citations
55	Fault analysis-resistant implementation of Rainbow Signature scheme. , 2017, , .		1
56	Detection of false data injection in automatic generation control systems using Kalman filter. , 2017, , .		24
57	Lelantos: A Blockchain-Based Anonymous Physical Delivery System. , 2017, , .		23
58	Improved Multiple Impossible Differential Cryptanalysis of Midori128. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1733-1737.	0.3	1
59	A Meet in the Middle Attack on Reduced Round Kiasu-BC. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 1888-1890.	0.3	7
60	Ultra-Dense Networks: A Survey. IEEE Communications Surveys and Tutorials, 2016, 18, 2522-2545.	39.4	747
61	Multiple association in ultra-dense networks. , 2016, , .		33
62	A Meet-in-the-Middle Attack on Reduced-Round Kalyna-<i>b</i>/2<i>b</i>. IEICE Transactions on Information and Systems, 2016, E99.D, 1246-1250.	0.7	4
63	Generalized MitM attacks on full TWINE. Information Processing Letters, 2016, 116, 128-135.	0.6	1
64	Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. IEEE Access, 2016, 4, 959-979.	4.2	109
65	Meet-in-the-Middle Attacks on Reduced Round Piccolo. Lecture Notes in Computer Science, 2016, , 3-20.	1.3	5
66	Watch your constants: malicious Streebog. IET Information Security, 2015, 9, 328-333.	1.7	7
67	A Meet in the Middle Attack on Reduced Round Kuznyechik. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 2194-2198.	0.3	9
68	Detection of malicious payload distribution channels in DNS. , 2014, , .		31
69	Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks. Journal of Cryptographic Engineering, 2013, 3, 227-240.	1.8	13
70	A Markov Decision Process Model for High Interaction Honeypots. Information Security Journal, 2013, 22, 159-170.	1.9	17
71	A game theoretic investigation for high interaction honeypots. , 2012, , .		9
72	Dempster-Shafer Evidence Combining for (Anti)-Honeypot Technologies. Information Security Journal, 2012, 21, 306-316.	1.9	12

#	Article	IF	Citations
73	On the Weak State in GGHN-like Ciphers. , 2012, , .		1
74	A Scan-Based Side Channel Attack on the NTRUEncrypt Cryptosystem. , 2012, , .		16
75	A Water-Filling Based Scheduling Algorithm for the Smart Grid. IEEE Transactions on Smart Grid, 2012, 3, 710-719.	9.0	81
76	Cryptanalysis of a key exchange protocol based on the endomorphisms ring End $${(mathbb{Z}_{p}) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 23, 143-149.	0.5	10
77	Fault analysis of the NTRUSign digital signature scheme. Cryptography and Communications, 2012, 4, 131-144.	1.4	11
78	Cryptanalysis of a <i>GL</i>(<i>r</i>,Z<i>_n</i>)-Based Public Key System. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95.A, 829-831.	0.3	0
79	Cryptanalysis of a public key cryptosystem based on boolean permutations. Journal of Discrete Mathematical Sciences and Cryptography, 2011, 14, 107-115.	0.8	0
80	Cryptanalysis of a Public Key Encryption Scheme Using Ergodic Matrices. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 853-854.	0.3	1
81	Fault Analysis of the NTRUEncrypt Cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1156-1158.	0.3	10
82	Cryptanalysis of Hwang-Lo-Hsiao-Chu Authenticated Encryption Schemes. IEICE Transactions on Information and Systems, 2010, E93-D, 1301-1302.	0.7	4
83	On the structural weakness of the GGHN stream cipher. Cryptography and Communications, 2010, 2, 1-17.	1.4	2
84	Joint Iterative Channel Estimation and Data Detection for MIMO-CDMA Systems over Frequency-Selective Fading Channels. , 2010, , .		0
85	Enhanced implementation of the NTRUEncrypt algorithm using graphics cards. , 2010, , .		4
86	A framework to strengthen password authentication using mobile devices and browser extensions. , 2010, , .		0
87	Applications of SAT Solvers to AES Key Recovery from Decayed Key Schedule Images. , 2010, , .		20
88	EM Channel Estimation and Data Detection for MIMO-CDMA Systems over Slow-Fading Channels. , 2010, , .		0
89	On the Existence of $(10, 2, 7, 488)$ Resilient Functions. IEEE Transactions on Information Theory, 2009, 55, 411-412.	2.4	9
90	A new distinguishing and key recovery attack on NGG stream cipher. Cryptography and Communications, 2009, 1, 269-282.	1.4	2

#	Article	IF	Citations
91	A rotary PIN entry scheme resilient to shoulder-surfing. , 2009, , .		3
92	An FPGA implementation of the NTRUEncrypt cryptosystem. , 2009, , .		32
93	On Reducing Blocking Probability in Cooperative Ad-hoc Networks. , 2009, , .		2
94	An FPGA implementation of AES with fault analysis countermeasures. , 2009, , .		2
95	An area-optimized implementation for AES with hybrid countermeasures against power analysis. , 2009, , .		3
96	A PIN Entry Scheme Resistant to Recording-Based Shoulder-Surfing. , 2009, , .		12
97	Performance of a MANET directional MAC protocol with angle-of-arrival estimation. Wireless Communications and Mobile Computing, 2008, 8, 759-769.	1.2	9
98	On the Security of a Cryptosystem Based on Multiple-Parameters Discrete Fractional Fourier Transform. IEEE Signal Processing Letters, 2008, 15, 77-78.	3.6	32
99	A Related-Key Attack on TREYFER. , 2008, , .		1
100	An Attack Against the Revised Murthyâ€“Swamy Cryptosystem. IEEE Transactions on Circuits and Systems II: Express Briefs, 2008, 55, 166-167.	3.0	4
101	An area optimized implementation of the Advanced Encryption Standard. , 2008, , .		5
102	On the nonlinearity profile of cryptographic Boolean functions. Canadian Conference on Electrical and Computer Engineering, 2008, , .	0.0	3
103	Space-time spreading and diversity in asynchronous CDMA systems over frequency-selective fading channels. , 2007, , .		0
104	Cryptanalysis of Pointcheval’s identification scheme using ant colony optimization. , 2007, , .		2
105	A Directional Routing Protocol for Ad Hoc Networks with Angle-of-Arrival Estimation. , 2007, , .		1
106	Incremental Hessian Locally Linear Embedding algorithm. , 2007, , .		6
107	Incremental Line Tangent Space Alignment Algorithm. , 2007, , .		6
108	An FPGA implementation of AES with support for counter and feedback modes. , 2007, , .		1

#	Article	IF	Citations
109	A Comment on “Cryptographic Applications of Brahmagupta–Bhãskara Equation”. IEEE Transactions on Circuits and Systems Part 1: Regular Papers, 2007, 54, 927-928.	0.1	10
110	WSN07-5: Performance of Directional MAC Protocols in Ad-Hoc Networks over Fading Channels. IEEE Global Telecommunications Conference (GLOBECOM), 2006, , .	0.0	0