

# Fagen Li

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/616921/publications.pdf>

Version: 2024-02-01

161  
papers

3,252  
citations

147801

31  
h-index

206112

48  
g-index

162  
all docs

162  
docs citations

162  
times ranked

2111  
citing authors

#	ARTICLE	IF	CITATIONS
1	Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things. IEEE Sensors Journal, 2013, 13, 3677-3684.	4.7	160
2	A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access, 2019, 7, 118943-118953.	4.2	134
3	An efficient certificateless aggregate signature with constant pairing computations. Information Sciences, 2013, 219, 225-235.	6.9	131
4	Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. Vehicular Communications, 2019, 16, 45-61.	4.0	120
5	Practical access control for sensor networks in the context of the Internet of Things. Computer Communications, 2016, 89-90, 154-164.	5.1	85
6	A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. Journal of Systems Architecture, 2019, 99, 101636.	4.3	85
7	An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. Journal of Systems Architecture, 2020, 103, 101692.	4.3	71
8	Secure and efficient data transmission in the Internet of Things. Telecommunication Systems, 2016, 62, 111-122.	2.5	68
9	An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Vehicular Communications, 2020, 22, 100228.	4.0	68
10	A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. Journal of Systems Architecture, 2020, 102, 101653.	4.3	67
11	Cost-Effective and Anonymous Access Control for Wireless Body Area Networks. IEEE Systems Journal, 2018, 12, 747-758.	4.6	64
12	Remote Authentication Schemes for Wireless Body Area Networks Based on the Internet of Things. IEEE Internet of Things Journal, 2018, 5, 4926-4944.	8.7	55
13	Efficient Signcryption for Heterogeneous Systems. IEEE Systems Journal, 2013, 7, 420-429.	4.6	53
14	An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid. Journal of Systems Architecture, 2019, 98, 165-172.	4.3	52
15	An Efficient Hybrid Signcryption Scheme With Conditional Privacy-Preservation for Heterogeneous Vehicular Communication in VANETs. IEEE Transactions on Vehicular Technology, 2020, 69, 11266-11280.	6.3	51
16	Certificateless authenticated key agreement for blockchain-based WBANs. Journal of Systems Architecture, 2020, 110, 101777.	4.3	51
17	Large universe attribute based access control with efficient decryption in cloud storage system. Journal of Systems and Software, 2018, 135, 157-164.	4.5	50
18	Identity-based broadcast signcryption. Computer Standards and Interfaces, 2008, 30, 89-94.	5.4	49

#	ARTICLE	IF	CITATIONS
19	Public-key authenticated encryption with keyword search achieving both multi-ciphertext and multi-trapdoor indistinguishability. <i>Journal of Systems Architecture</i> , 2021, 115, 102075.	4.3	45
20	A Secure ECC-based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety. <i>Journal of Medical Systems</i> , 2016, 40, 12.	3.6	44
21	Efficient certificateless access control for industrial Internet of Things. <i>Future Generation Computer Systems</i> , 2017, 76, 285-292.	7.5	43
22	Efficient and multi-level privacy-preserving communication protocol for VANET. <i>Computers and Electrical Engineering</i> , 2012, 38, 573-581.	4.8	42
23	Efficient Certificateless Access Control for Wireless Body Area Networks. <i>IEEE Sensors Journal</i> , 2016, 16, 5389-5396.	4.7	41
24	Certificateless online/offline signcryption for the Internet of Things. <i>Wireless Networks</i> , 2017, 23, 145-158.	3.0	41
25	AKAloTs: authenticated key agreement for Internet of Things. <i>Wireless Networks</i> , 2019, 25, 3081-3101.	3.0	38
26	Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. <i>Journal of Medical Systems</i> , 2018, 42, 108.	3.6	37
27	Identity-based deniable authentication for ad hoc networks. <i>Computing (Vienna/New York)</i> , 2014, 96, 843-853.	4.8	36
28	Practical Signcryption for Secure Communication of Wireless Sensor Networks. <i>Wireless Personal Communications</i> , 2016, 89, 1391-1412.	2.7	35
29	Efficient Signcryption With Proxy Re-Encryption and its Application in Smart Grid. <i>IEEE Internet of Things Journal</i> , 2019, 6, 9722-9737.	8.7	33
30	Certificateless hybrid signcryption. <i>Mathematical and Computer Modelling</i> , 2013, 57, 324-343.	2.0	32
31	An efficient certificateless public key encryption scheme with authorized equality test in healthcare environments. <i>Journal of Systems Architecture</i> , 2020, 109, 101776.	4.3	32
32	A cloud data deduplication scheme based on certificateless proxy re-encryption. <i>Journal of Systems Architecture</i> , 2020, 102, 101666.	4.3	31
33	A Blockchain-Based Privacy-Awareness Authentication Scheme With Efficient Revocation for Multi-Server Architectures. <i>IEEE Access</i> , 2019, 7, 125840-125853.	4.2	31
34	An Efficient Remote Authentication Scheme for Wireless Body Area Network. <i>Journal of Medical Systems</i> , 2017, 41, 25.	3.6	30
35	Bidder-anonymous English auction protocol based on revocable ring signature. <i>Expert Systems With Applications</i> , 2012, 39, 7062-7066.	7.6	29
36	HOOSC: heterogeneous online/offline signcryption for the Internet of Things. <i>Wireless Networks</i> , 2018, 24, 3141-3160.	3.0	29

#	ARTICLE	IF	CITATIONS
37	An efficient signcryption for data access control in cloud computing. <i>Computing (Vienna/New York)</i> , 2017, 99, 465-479.	4.8	28
38	IBEET-RSA: Identity-Based Encryption with Equality Test over RSA for Wireless Body Area Networks. <i>Mobile Networks and Applications</i> , 2020, 25, 223-233.	3.3	25
39	An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks. <i>Journal of Systems Architecture</i> , 2021, 119, 102271.	4.3	25
40	Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model. <i>Security and Communication Networks</i> , 2013, 6, 69-77.	1.5	24
41	Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement. <i>Computer Standards and Interfaces</i> , 2018, 56, 101-106.	5.4	24
42	Identity-based online/offline signcryption for low power devices. <i>Journal of Network and Computer Applications</i> , 2012, 35, 340-347.	9.1	23
43	An efficient certificateless user authentication and key exchange protocol for client-server environment. <i>Journal of Ambient Intelligence and Humanized Computing</i> , 2018, 9, 1713-1727.	4.9	23
44	Authenticated key agreement for blockchain-based WBAN. <i>Telecommunication Systems</i> , 2020, 74, 347-365.	2.5	23
45	An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks. <i>Lecture Notes in Computer Science</i> , 2007, , 373-384.	1.3	23
46	Practical Identity-Based Signature for Wireless Sensor Networks. <i>IEEE Wireless Communications Letters</i> , 2012, 1, 637-640.	5.0	22
47	Secure identity-based signcryption in the standard model. <i>Mathematical and Computer Modelling</i> , 2013, 57, 2685-2694.	2.0	22
48	Lattice-based signcryption. <i>Concurrency Computation Practice and Experience</i> , 2013, 25, 2112-2122.	2.2	21
49	An Improved Two-Layer Authentication Scheme for Wireless Body Area Networks. <i>Journal of Medical Systems</i> , 2018, 42, 143.	3.6	21
50	An efficient and practical certificateless signcryption scheme for wireless body area networks. <i>Computer Communications</i> , 2020, 162, 169-178.	5.1	21
51	A Provably-Secure Transmission Scheme for Wireless Body Area Networks. <i>Journal of Medical Systems</i> , 2016, 40, 247.	3.6	20
52	Practical deniable authentication for pervasive computing environments. <i>Wireless Networks</i> , 2018, 24, 139-149.	3.0	20
53	Efficient Deniably Authenticated Encryption and Its Application to E-Mail. <i>IEEE Transactions on Information Forensics and Security</i> , 2016, 11, 2477-2486.	6.9	19
54	Certificateless public key encryption with cryptographic reverse firewalls. <i>Journal of Systems Architecture</i> , 2020, 109, 101754.	4.3	19

#	ARTICLE	IF	CITATIONS
55	Leakage-Free and Provably Secure Certificateless Signcryption Scheme Using Bilinear Pairings. Computer Journal, 2015, 58, 2636-2648.	2.4	18
56	A combined public-key scheme in the case of attribute-based for wireless body area networks. Wireless Networks, 2019, 25, 845-859.	3.0	18
57	A Provably Secure Proxy Signature Scheme in Certificateless Cryptography. Informatica, 2010, 21, 277-294.	2.7	18
58	A Survey of Identity-based Signcryption. IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), 2010, 27, 214.	3.2	17
59	A biometric identity-based signcryption scheme. Future Generation Computer Systems, 2012, 28, 306-310.	7.5	17
60	A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing. Sensors, 2020, 20, 4720.	3.8	17
61	On the security of an identity based multi-proxy signature scheme. Computers and Electrical Engineering, 2011, 37, 129-135.	4.8	16
62	A Blockchain-Based Access Control Scheme for Smart Grids. , 2019, , .		16
63	Quantum public-key designated verifier signature. Quantum Information Processing, 2022, 21, 1.	2.2	16
64	Heterogeneous signcryption with keyword search for wireless body area network. Security and Privacy, 2018, 1, e25.	2.7	15
65	Identity-Based Combined Public Key Schemes for Signature, Encryption, and Signcryption. Advances in Intelligent Systems and Computing, 2019, , 3-22.	0.6	15
66	Identity-Based User Authenticated Key Agreement Protocol for Multi-Server Environment with Anonymity. Mobile Networks and Applications, 2019, 24, 890-902.	3.3	15
67	ID-based threshold proxy signcryption scheme from bilinear pairings. International Journal of Security and Networks, 2008, 3, 206.	0.2	14
68	Image spam classification based on low-level image features. , 2010, , .		14
69	Analysis of an Identity-Based Signcryption Scheme in the Standard Model. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 268-269.	0.3	14
70	Cryptanalysis and Improvement of Robust Deniable Authentication Protocol. Wireless Personal Communications, 2013, 69, 1391-1398.	2.7	14
71	Certificateless threshold signature secure in the standard model. Information Sciences, 2013, 237, 73-81.	6.9	14
72	Secure Vehicle-to-roadside Communication Protocol Using Certificate-based Cryptosystem. IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), 2010, 27, 214.	3.2	13

#	ARTICLE	IF	CITATIONS
73	Efficient privacy-preserving authentication protocol for vehicular communications with trustworthy. Security and Communication Networks, 2012, 5, 1441-1451.	1.5	13
74	Identity-based partially blind signature in the standard model for electronic cash. Mathematical and Computer Modelling, 2013, 58, 196-203.	2.0	13
75	Certificateless public key encryption with conjunctive keyword search and its application to cloud-based reliable smart grid system. Annales Des Telecommunications/Annals of Telecommunications, 2019, 74, 435-449.	2.5	13
76	Searchable Public-Key Encryption With Cryptographic Reverse Firewalls for Cloud Storage. IEEE Transactions on Cloud Computing, 2023, 11, 383-396.	4.4	13
77	An Improved Identity-Based KCDSA Signcryption Scheme. , 2007, , .		12
78	A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems. Symmetry, 2016, 8, 85.	2.2	12
79	Identity-based deniable authenticated encryption and its application to e-mail system. Telecommunication Systems, 2016, 62, 625-639.	2.5	12
80	Identity-Based Auditing for Shared Cloud Data With Efficient and Secure Sensitive Information Hiding. IEEE Access, 2019, 7, 114246-114260.	4.2	12
81	New Public-key Quantum Signature Scheme with Quantum One-Way Function. International Journal of Theoretical Physics, 2019, 58, 3282-3294.	1.2	12
82	An Efficient Privacy-Aware Authentication Scheme With Hierarchical Access Control for Mobile Cloud Computing Services. IEEE Transactions on Cloud Computing, 2022, 10, 2309-2323.	4.4	12
83	Toward Invisible Adversarial Examples Against DNN-Based Privacy Leakage for Internet of Things. IEEE Internet of Things Journal, 2021, 8, 802-812.	8.7	12
84	On the Security of Online/Offline Signatures and Multisignatures from ACISP'06. Lecture Notes in Computer Science, 2008, , 108-119.	1.3	12
85	A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid. Telecommunication Systems, 2019, 70, 491-510.	2.5	11
86	A heterogeneous user authentication and key establishment for mobile client-server environment. Wireless Networks, 2020, 26, 913-924.	3.0	11
87	Efficient and provably secure multi-recipient signcryption from bilinear pairings. Wuhan University Journal of Natural Sciences, 2007, 12, 17-20.	0.4	10
88	Provably secure and efficient certificateless authenticated tripartite key agreement protocol. Mathematical and Computer Modelling, 2012, 55, 1213-1221.	2.0	10
89	Analysis of an ABE Scheme with Verifiable Outsourced Decryption. Sensors, 2018, 18, 176.	3.8	10
90	Certificateless deniably authenticated encryption and its application to e-voting system. Telecommunication Systems, 2019, 70, 417-434.	2.5	10

#	ARTICLE	IF	CITATIONS
91	Efficient arbitrated quantum signature scheme without entangled states. <i>Modern Physics Letters A</i> , 2019, 34, 1950166.	1.2	10
92	Identity-Based Signature With Server-Aided Verification Scheme for 5G Mobile Systems. <i>IEEE Access</i> , 2020, 8, 51810-51820.	4.2	10
93	Quantum public-key signature scheme based on asymmetric quantum encryption with trapdoor information. <i>Quantum Information Processing</i> , 2020, 19, 1.	2.2	10
94	A Lightweight Anonymous Authentication Protocol for Resource-Constrained Devices in Internet of Things. <i>IEEE Internet of Things Journal</i> , 2022, 9, 1818-1829.	8.7	10
95	Analysis and improvement of authenticatable ring signcryption scheme. <i>Journal of Shanghai Jiaotong University (Science)</i> , 2008, 13, 679-683.	0.9	9
96	Insecurity of A Key-Policy Attribute Based Encryption Scheme With Equality Test. <i>IEEE Access</i> , 2018, 6, 10189-10196.	4.2	9
97	Identity-Based Quantum Designated Verifier Signature. <i>International Journal of Theoretical Physics</i> , 2020, 59, 918-929.	1.2	9
98	Efficient Identity-Based Signcryption in the Standard Model. <i>Lecture Notes in Computer Science</i> , 2011, , 120-137.	1.3	9
99	An Efficient Identity-Based Deniable Authenticated Encryption Scheme. <i>KSII Transactions on Internet and Information Systems</i> , 2015, 9, .	0.3	9
100	An efficient certificateless deniable authentication protocol without pairings. <i>International Journal of Electronic Security and Digital Forensics</i> , 2015, 7, 179.	0.2	8
101	Quantum designated verifier signature based on Bell states. <i>Quantum Information Processing</i> , 2020, 19, 1.	2.2	8
102	ID-Based Threshold Unsigncryption Scheme from ID Pairings. <i>Lecture Notes in Computer Science</i> , 2005, , 242-253.	1.3	8
103	Key Management Using Certificateless Public Key Cryptography in Ad Hoc Networks. <i>Lecture Notes in Computer Science</i> , 2008, , 116-126.	1.3	8
104	A Pairing-Free Heterogeneous Signcryption Scheme for Unmanned Aerial Vehicles. <i>IEEE Internet of Things Journal</i> , 2022, 9, 19426-19437.	8.7	8
105	An efficient identity-based anonymous signcryption scheme. <i>Wuhan University Journal of Natural Sciences</i> , 2008, 13, 670-674.	0.4	7
106	Efficient communication scheme with confidentiality and privacy for vehicular networks. <i>Computers and Electrical Engineering</i> , 2013, 39, 1717-1725.	4.8	7
107	Multi-User Searchable Symmetric Encryption with Dynamic Updates for Cloud Computing. <i>Information (Switzerland)</i> , 2018, 9, 242.	2.9	7
108	Digital signature with cryptographic reverse firewalls. <i>Journal of Systems Architecture</i> , 2021, 116, 102029.	4.3	7

#	ARTICLE	IF	CITATIONS
109	A Certificateless Proxy Re-encryption Scheme for Cloud-Based Blockchain. Communications in Computer and Information Science, 2019, , 293-307.	0.5	7
110	Identity-Based Hybrid Signcryption. , 2009, , .		6
111	Secure mobile health system supporting search function and decryption verification. Journal of Ambient Intelligence and Humanized Computing, 2021, 12, 2221-2231.	4.9	6
112	Efficient Multi-PKG ID-Based Signcryption for Ad Hoc Networks. Lecture Notes in Computer Science, 2009, , 289-304.	1.3	6
113	An efficient ID-based ring signcryption scheme. , 2008, , .		5
114	Further improvement of an identity-based signcryption scheme in the standard model. Computers and Electrical Engineering, 2012, 38, 413-421.	4.8	5
115	An efficient end-to-end mutual authentication scheme for 2G-GSM system. , 2016, , .		5
116	Quantum proxy signature with provable security. Modern Physics Letters A, 2020, 35, 2050197.	1.2	5
117	An HMAC-based authentication scheme for network coding with support for error correction and rogue node identification. Journal of Systems Architecture, 2021, 116, 102051.	4.3	5
118	Efficient Signcryption Key Encapsulation without Random Oracles. Lecture Notes in Computer Science, 2009, , 47-59.	1.3	5
119	A provably secure free-pairing certificateless searchable encryption scheme. Telecommunication Systems, 2022, 80, 383-395.	2.5	5
120	An efficient and provably secure ID-based threshold signcryption scheme. , 2008, , .		4
121	A new multi-receiver ID-based signcryption scheme for group communications. , 2009, , .		4
122	Cryptanalysis of efficient proxy signature schemes for mobile communication. Science China Information Sciences, 2010, 53, 2016-2021.	4.3	4
123	An Improved Authenticated Encryption Scheme. IEICE Transactions on Information and Systems, 2011, E94-D, 2171-2172.	0.7	4
124	Black Box Traceable Ciphertext Policy Attribute-Based Encryption Scheme. Information (Switzerland), 2015, 6, 481-493.	2.9	4
125	Authentication and key agreement scheme for CDMA cellular system. , 2015, , .		4
126	ASDS: Attribute-based secure data sharing scheme for reliable cloud environment. Security and Privacy, 2019, 2, e57.	2.7	4



#	ARTICLE	IF	CITATIONS
127	Provably Secure Identity-Based Threshold Unsignryption Scheme. Lecture Notes in Computer Science, 2007, , 114-122.	1.3	4
128	Certificateless Authenticated Key Agreement for Decentralized WBANs. Communications in Computer and Information Science, 2019, , 268-290.	0.5	4
129	Identity Based Multi-proxy Multi-signryption Scheme for Electronic Commerce. , 2009, , .		3
130	A novel certificateless deniable authentication protocol. International Journal of Computers and Applications, 2015, 37, 181-192.	1.3	3
131	Ciphertext retrieval against insider attacks for cloud storage. , 2016, , .		3
132	A public key encryption scheme based on a new variant of LWE with small cipher size. Journal of Systems Architecture, 2021, 117, 102165.	4.3	3
133	A computationally efficient HMAC-based authentication scheme for network coding. Telecommunication Systems, 2022, 79, 47-69.	2.5	3
134	Certificateless Authentication and Consensus for the Blockchain-Based Smart Grid. Communications in Computer and Information Science, 2022, , 134-151.	0.5	3
135	Cryptanalysis of a convertible authenticated encryption scheme based on the ElGamal cryptosystem. IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), 2010, 27, 266.	3.2	2
136	Efficient signryption in the standard model. Concurrency Computation Practice and Experience, 2012, 24, 1977-1989.	2.2	2
137	A taxonomy of ring signature schemes: Theory and applications. IETE Journal of Research, 2013, 59, 376.	2.6	2
138	Compact Leakage-Free ID-Based Signature Scheme with Applications to Secret Handshakes. Wireless Personal Communications, 2015, 80, 1671-1685.	2.7	2
139	Modeling and Solving Scheduling in Overloaded Situations with Weighted Partial MaxSAT. Mathematical Problems in Engineering, 2021, 2021, 1-17.	1.1	2
140	EEE-GSM: End-to-End Encryption Scheme over GSM System. International Journal of Security and Its Applications, 2016, 10, 229-240.	0.8	2
141	Cryptanalysis of Strong Designated Verifier Signature Scheme with Non-delegatability and Non-transferability. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 259-262.	0.3	2
142	Simulatability and Security of Certificateless Threshold Signatures without Random Oracles. , 2008, , .		1
143	Deniable Proxy-Anonymous Signatures. , 2008, , .		1
144	Improvement of A proactive Threshold Signryption Scheme. International Journal of Computers and Applications, 2008, 30, 345-347.	1.3	1

#	ARTICLE	IF	CITATIONS
145	A generic construction of identity-based signcryption. , 2009, , .		1
146	Security Analysis and Improvement of Pairing-Based Threshold Proxy Signature Scheme. , 2009, , .		1
147	New Signcryption from q-Diffie-Hellman Problems. , 2010, , .		1
148	Cryptanalysis of an Identity Based Signcryption without Random Oracles. Fundamenta Informaticae, 2011, 107, 105-109.	0.4	1
149	Analysis and Improvement of a Secret Broadcast with Binding Encryption in Broadcasting Networks. IEICE Transactions on Information and Systems, 2012, E95-D, 686-689.	0.7	1
150	Security Flaw of an Improved User Authentication Scheme with User Anonymity for Wireless Communications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 256-258.	0.3	1
151	An Anonymous Multireceiver with Online/Offline Identity-Based Encryption. Wireless Communications and Mobile Computing, 2018, 2018, 1-10.	1.2	1
152	Comments on an identity-based signature scheme for VANETs. Journal of Systems Architecture, 2021, 112, 101851.	4.3	1
153	Linearization Equation Attack on 2-Layer Nonlinear Piece in Hand Method. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 1952-1961.	0.3	1
154	Improvement on a Knapsack-Based Probabilistic Encryption Scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 421-424.	0.3	1
155	A heterogeneous authenticated key establishment protocol for Internet of drones. , 2021, , .		1
156	ID-Based (t, n) Threshold Proxy Signcryption for Multi-Agent Systems. , 2006, , .		0
157	ID-Based Deniable Threshold Ring Authentication. , 2015, , .		0
158	Secure mobile agent-based English auction protocol using identity-based signature scheme. International Journal of Security and Networks, 2016, 11, 175.	0.2	0
159	CLIBDA: A Deniable Authentication Scheme for Pervasive Computing Environment. Communications in Computer and Information Science, 2019, , 67-83.	0.5	0
160	A Lightweight Certificateless User Authentication Scheme for Mobile Environment. Lecture Notes in Computer Science, 2019, , 112-122.	1.3	0
161	A Secure User Authentication Protocol for Heterogeneous Mobile Environments. IEEE Access, 2022, 10, 69757-69770.	4.2	0