De-biao He

List of Publications by Citations

264	9,408	53	90
papers	citations	h-index	g-index
276	11,552	4.1	7.26
ext. papers	ext. citations	avg, IF	L-index

#	Paper	IF	Citations
264	An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 2681-2691	8	465
263	A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, **2019**, 126, 45-58	7.9	302
262	Robust Biometrics-Based Authentication Scheme for Multiserver Environment. *IEEE Systems Journal*, **2015**, 9, 816-823	4.3	286
261	Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. *IEEE Transactions on Dependable and Secure Computing*, **2015**, 12, 428-442	3.9	276
260	Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, **2019**, 135, 62-75	7.9	271
259	Anonymous Authentication for Wireless Body Area Networks With Provable Security. *IEEE Systems Journal*, **2017**, 11, 2590-2601	4.3	248
258	BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications*, **2018**, 116, 42-52	7.9	212
257	Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, **2015**, 21, 49-60	2.2	211
256	Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access*, **2017**, 5, 3376-3392	3.5	198
255	A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, **2012**, 36, 1989-95	5.1	196
254	An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet of Things Journal*, **2015**, 2, 72-83	10.7	178
253	A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences*, **2015**, 321, 263-277	7.7	177
252	Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Communications Magazine*, **2018**, 56, 64-69	9.1	159
251	Authentication protocol for an ambient assisted living system **2015**, 53, 71-77		159
250	Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks. *IEEE Systems Journal*, **2018**, 12, 64-73	4.3	147
249	Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 759-767	11.9	144
248	An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security. *Information Fusion*, **2012**, 13, 223-230	16.7	142

247	A privacy preserving three-factor authentication protocol for e-Health clouds. *Journal of Supercomputing*, **2016**, 72, 3826-3849	2.5	135
246	Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Transactions on Consumer Electronics*, **2014**, 60, 30-37	4.8	135
245	Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries. *IEEE Transactions on Smart Grid*, **2017**, 8, 2411-2419	10.7	124
244	Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures. *IEEE Transactions on Information Forensics and Security* , **2016**, 11, 2052-2064	8	117
243	Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1165-1176	8	115
242	Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 3618-3627	11.9	102
241	Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. *IEEE Systems Journal*, **2018**, 12, 1621-1631	4.3	97
240	Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 16, 996-1010	3.9	97
239	Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. *Nonlinear Dynamics*, **2012**, 69, 1149-1157	5	95
238	Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems*, **2018**, 89, 110-125	7.5	94
237	Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers and Security*, **2020**, 97, 101966	4.9	92
236	An efficient and provably-secure certificateless signature scheme without bilinear pairings. *International Journal of Communication Systems*, **2012**, 25, 1432-1442	1.7	88
235	BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 4146-4155	11.9	88
234	Authenticated key agreement scheme for fog-driven IoT healthcare system. *Wireless Networks*, **2019**, 25, 4737-4750	2.5	86
233	Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 1984-1992	11.9	86
232	Privacy-preserving data aggregation scheme against internal attackers in smart grids. *Wireless Networks*, **2016**, 22, 491-502	2.5	85
231	A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. *IEEE Transactions on Dependable and Secure Computing*, **2018**, 15, 633-645	3.9	83
230	. *IEEE Systems Journal*, **2018**, 12, 916-925	4.3	80

229	Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. *IET Communications*, **2016**, 10, 1795-1802	1.3	80
228	Secure Key Agreement and Key Protection for Mobile Device User Authentication. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 319-330	8	79
227	An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings. *Ad Hoc Networks*, **2012**, 10, 1009-1016	4.8	74
226	Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems*, **2014**, 38, 116	5.1	71
225	A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. *Security and Communication Networks*, **2012**, 5, 1423-1429	1.9	71
224	A pairing-free certificateless authenticated key agreement protocol. *International Journal of Communication Systems*, **2012**, 25, 221-230	1.7	68
223	HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. *IEEE Internet of Things Journal*, **2020**, 7, 818-829	10.7	65
222	A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing. *IEEE Systems Journal*, **2020**, 14, 560-571	4.3	64
221	Efficient and secure identity-based encryption scheme with equality test in cloud computing. *Future Generation Computer Systems*, **2017**, 73, 22-31	7.5	63
220	An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. *IEEE Internet of Things Journal*, **2019**, 6, 8065-8075	10.7	63
219	Anonymous two-factor authentication for consumer roaming service in global mobility networks. *IEEE Transactions on Consumer Electronics*, **2013**, 59, 811-817	4.8	62
218	New biometrics-based authentication scheme for multi-server environment in critical systems. *Journal of Ambient Intelligence and Humanized Computing*, **2015**, 6, 825-834	3.7	57
217	A lightweight authentication and key agreement scheme for Internet of Drones. *Computer Communications*, **2020**, 154, 455-464	5.1	57
216	An ID-based proxy signature schemes without bilinear pairings. *Annales Des Telecommunications/Annals of Telecommunications*, **2011**, 66, 657-662	2	57
215	Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. *Future Generation Computer Systems*, **2018**, 84, 239-251	7.5	57
214	One-to-many authentication for access control in mobile pay-TV systems. *Science China Information Sciences*, **2016**, 59, 1	3.4	55
213	Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, **2020**, 166, 102731	7.9	53
212	Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network. *IEEE Transactions on Vehicular Technology*, **2019**, 68, 11309-11322	6.8	53

211	Insecurity of an efficient certificateless aggregate signature with constant pairing computations. *Information Sciences*, **2014**, 268, 458-462	7.7	52
210	Cryptanalysis and Improvement of an Anonymous Authentication Protocol for Wireless Access Networks. *Wireless Personal Communications*, **2014**, 74, 229-243	1.9	51
209	Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 1232-1241	11.9	50
208	DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments. *IEEE Transactions on Computers*, **2016**, 65, 3631-3645	2.5	49
207	Incentive and Unconditionally Anonymous Identity-Based Public Provable Data Possession. *IEEE Transactions on Services Computing*, **2019**, 12, 824-835	4.8	49
206	An efficient certificateless two-party authenticated key agreement protocol. *Computers and Mathematics With Applications*, **2012**, 64, 1914-1926	2.7	48
205	DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 2440-2452	8	46
204	An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment. *Ad Hoc Networks*, **2018**, 71, 78-87	4.8	46
203	Blind Filtering at Third Parties: An Efficient Privacy-Preserving Framework for Location-Based Services. *IEEE Transactions on Mobile Computing*, **2018**, 17, 2524-2535	4.6	46
202	Security Flaws in a Smart Card Based Authentication Scheme for Multi-server Environment. *Wireless Personal Communications*, **2013**, 70, 323-329	1.9	44
201	A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. *IEEE Access*, **2018**, 6, 28203-28212	3.5	44
200	New certificateless short signature scheme. *IET Information Security*, **2013**, 7, 113-117	1.4	43
199	A new two-round certificateless authenticated key agreement protocol without bilinear pairings. *Mathematical and Computer Modelling*, **2011**, 54, 3143-3152		42
198	Certificateless searchable public key encryption scheme for mobile healthcare system. *Computers and Electrical Engineering*, **2018**, 65, 413-424	4.3	41
197	BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Transactions on Intelligent Transportation Systems*, **2020**, 1-13	6.1	40
196	Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks. *IEEE Transactions on Mobile Computing*, **2017**, 16, 1530-1543	4.6	40
195	Efficient Hierarchical Identity-Based Signature With Batch Verification for Automatic Dependent Surveillance-Broadcast System. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 454-464	8	39
194	Dominating Set and Network Coding-Based Routing in Wireless Mesh Networks. *IEEE Transactions on Parallel and Distributed Systems*, **2015**, 26, 423-433	3.7	38

193	Privacy-preserving certificateless provable data possession scheme for big data storage on cloud. *Applied Mathematics and Computation*, **2017**, 314, 31-43	2.7	38
192	BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT. *Wireless Communications and Mobile Computing*, **2018**, 2018, 1-9	1.9	38
191	Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing. *Soft Computing*, **2017**, 21, 7325-7335	3.5	37
190	An efficient identity-based blind signature scheme without bilinear pairings. *Computers and Electrical Engineering*, **2011**, 37, 444-450	4.3	35
189	BBARS: Blockchain-Based Anonymous Rewarding Scheme for V2G Networks. *IEEE Internet of Things Journal*, **2019**, 6, 3676-3687	10.7	34
188	Efficient and secure searchable encryption protocol for cloud-based Internet of Things. *Journal of Parallel and Distributed Computing*, **2018**, 111, 152-161	4.4	32
187	Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation. *Science China Information Sciences*, **2017**, 60, 1	3.4	32
186	Blockchain-based system for secure outsourcing of bilinear pairings. *Information Sciences*, **2020**, 527, 590-601	7.7	32
185	An efficient certificateless proxy signature scheme without pairing. *Mathematical and Computer Modelling*, **2013**, 57, 2510-2518		31
184	Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices. *Soft Computing*, **2017**, 21, 6801-6810	3.5	30
183	Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. *Future Generation Computer Systems*, **2020**, 107, 854-862	7.5	30
182	. *IEEE Transactions on Sustainable Computing*, **2018**, 3, 44-55	3.5	29
181	A Survey of Blockchain Applications in the Energy Sector. *IEEE Systems Journal*, **2021**, 15, 3370-3381	4.3	28
180	. *IEEE Consumer Electronics Magazine*, **2019**, 8, 45-49	3.2	27
179	Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage. *Information Sciences*, **2017**, 375, 48-53	7.7	27
178	A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks. *IEEE Transactions on Vehicular Technology*, **2020**, 69, 5813-5825	6.8	27
177	New Certificateless Aggregate Signature Scheme for Healthcare Multimedia Social Network on Cloud Environment. *Security and Communication Networks*, **2018**, 2018, 1-13	1.9	25
176	Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices. *IEEE Systems Journal*, **2019**, 13, 2775-2785	4.3	25

175	An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography. *Wireless Personal Communications*, **2015**, 85, 225-240	1.9	25
174	A new handover authentication protocol based on bilinear pairing functions for wireless networks. *International Journal of Ad Hoc and Ubiquitous Computing*, **2015**, 18, 67	0.7	25
173	Secure and Efficient Two-Party Signing Protocol for the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 17, 1124-1132	3.9	25
172	Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. *Science China Information Sciences*, **2022**, 65, 1	3.4	25
171	Lightweight Data Aggregation Scheme against Internal Attackers in Smart Grid Using Elliptic Curve Cryptography. *Wireless Communications and Mobile Computing*, **2017**, 2017, 1-11	1.9	24
170	. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	24
169	Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things. *Annales Des Telecommunications/Annals of Telecommunications*, **2019**, 74, 423-434	2	24
168	VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud. *IEEE Transactions on Services Computing*, **2020**, 13, 572-583	4.8	24
167	An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. *IEEE Internet of Things Journal*, **2021**, 8, 458-473	10.7	24
166	Secure pseudonym-based near field communication protocol for the consumer internet of things. *IEEE Transactions on Consumer Electronics*, **2015**, 61, 56-62	4.8	23
165	Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol. *Information Sciences*, **2012**, 215, 83-96	7.7	23
164	A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. *International Journal of Network Management*, **2017**, 27, e1937	1.8	22
163	An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 641-651	3.9	22
162	Reattack of a certificateless aggregate signature scheme with constant pairing computations. *Scientific World Journal, The*, **2014**, 2014, 343715	2.2	21
161	SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system. *Science China Information Sciences*, **2020**, 63, 1	3.4	20
160	Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption. *Soft Computing*, **2018**, 22, 707-714	3.5	20
159	PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management. *IEEE Access*, **2019**, 7, 6117-6128	3.5	20
158	Efficient Revocable ID-Based Signature With Cloud Revocation Server. *IEEE Access*, **2017**, 5, 2945-2954	3.5	19

157	An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. *Soft Computing*, **2018**, 22, 7685-7696	3.5	19
156	Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. *Computer Networks*, **2017**, 128, 154-163	5.4	18
155	Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps. *Soft Computing* , **2018**, 22, 2267-2274	3.5	18
154	Lightweight Searchable Public-key Encryption with Forward Privacy over IIoT Outsourced Data. *IEEE Transactions on Emerging Topics in Computing*, **2019**, 1-1	4.1	18
153	. *IEEE Transactions on Intelligent Transportation Systems*, **2021**, 22, 3939-3951	6.1	18
152	A secure data backup scheme using multi-factor authentication. *IET Information Security*, **2017**, 11, 250-255	1.4	17
151	. *IEEE Internet of Things Journal*, **2020**, 7, 6056-6068	10.7	17
150	An Id-Based Three-Party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography for Mobile-Commerce Environments. *Arabian Journal for Science and Engineering*, **2013**, 38, 2055-2061		16
149	Improved secure fuzzy auditing protocol for cloud data storage. *Soft Computing*, **2019**, 23, 3411-3422	3.5	16
148	Anonymous and Efficient Message Authentication Scheme for Smart Grid. *Security and Communication Networks*, **2019**, 2019, 1-12	1.9	15
147	Note on Design of improved password authentication and update scheme based on elliptic curve cryptography *Mathematical and Computer Modelling*, **2012**, 55, 1661-1664		15
146	Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme. *IET Information Security*, **2020**, 14, 443-451	1.4	15
145	An efficient and provable certificate-based proxy signature scheme for IIoT environment. *Information Sciences*, **2020**, 518, 142-156	7.7	14
144	A new dynamic identity-based authentication protocol for multi-server environment using elliptic curve cryptography. *Security and Communication Networks*, **2012**, 5, 1260-1266	1.9	14
143	CB-PS: An Efficient Short-Certificate-Based Proxy Signature Scheme for UAVs. *IEEE Systems Journal*, **2020**, 14, 621-632	4.3	14
142	Human-in-the-Loop-Aided Privacy-Preserving Scheme for Smart Healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence*, **2020**, 1-10	4.1	13
141	Blockchain-Based Private Provable Data Possession. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 1-1	3.9	13
140	Dynamic Group-Oriented Provable Data Possession in the Cloud. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	13

139	Efficient provably secure password-based explicit authenticated key agreement. *Pervasive and Mobile Computing*, **2015**, 24, 50-60	3.5	12
138	Efficient Certificateless Aggregate Signature Scheme for Performing Secure Routing in VANETs. *Security and Communication Networks*, **2020**, 2020, 1-12	1.9	12
137	Signature-based three-factor authenticated key exchange for internet of things applications. *Multimedia Tools and Applications*, **2018**, 77, 18355-18382	2.5	12
136	Compact Hardware Implementation of a SHA-3 Core for Wireless Body Sensor Networks. *IEEE Access*, **2018**, 6, 40128-40136	3.5	12
135	Secure public data auditing scheme for cloud storage in smart city. *Personal and Ubiquitous Computing*, **2017**, 21, 949-962	2.1	12
134	A secure and efficient public auditing scheme using RSA algorithm for cloud storage. *Journal of Supercomputing*, **2017**, 73, 5285-5309	2.5	11
133	A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography. *International Journal of Communication Systems*, **2017**, 30, e3333	1.7	11
132	Efficient NTRU Lattice-Based Certificateless Signature Scheme for Medical Cyber-Physical Systems. *Journal of Medical Systems*, **2020**, 44, 92	5.1	11
131	Cryptanalysis and Improvement of a Password-Based Remote User Authentication Scheme without Smart Cards. *Information Technology and Control*, **2013**, 42,	1.3	11
130	Algebraic Signatures-Based Data Integrity Auditing for Efficient Data Dynamics in Cloud Computing. *IEEE Transactions on Sustainable Computing*, **2020**, 5, 161-173	3.5	11
129	OBFP: Optimized Blockchain-Based Fair Payment for Outsourcing Computations in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, **2021**, 16, 3241-3253	8	11
128	White-Box Implementation of the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. *IEICE Transactions on Information and Systems*, **2020**, E103.D, 188-195	0.6	10
127	Privacy-preserving auditing scheme for shared data in public clouds. *Journal of Supercomputing*, **2018**, 74, 6156-6183	2.5	10
126	Privacy-preserving incentive and rewarding scheme for crowd computing in social media. *Information Sciences*, **2019**, 470, 15-27	7.7	10
125	Dual-Server Public-Key Authenticated Encryption With Keyword Search. *IEEE Transactions on Cloud Computing*, **2019**, 1-1	3.3	10
124	Weaknesses of a dynamic ID-based remote user authentication scheme. *International Journal of Electronic Security and Digital Forensics*, **2010**, 3, 355	1	10
123	Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare. *Journal of Information Security and Applications*, **2020**, 50, 102429	3.5	10
122	The Application of the Blockchain Technology in Voting Systems. *ACM Computing Surveys*, **2021**, 54, 1-28	13.4	9

121	Blockchain-Based Anonymous Reporting Scheme With Anonymous Rewarding. *IEEE Transactions on Engineering Management*, **2020**, 67, 1514-1524	2.6	9
120	Efficient Identity-Based Distributed Decryption Scheme for Electronic Personal Health Record Sharing System. *IEEE Journal on Selected Areas in Communications*, **2021**, 39, 384-395	14.2	9
119	Blockchain-Based Secure and Lightweight Authentication for Internet of Things. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	9
118	Succinct multi-authority attribute-based access control for circuits with authenticated outsourcing. *Soft Computing*, **2017**, 21, 5265-5279	3.5	8
117	A security-enhanced authentication with key agreement scheme for wireless mobile communications using elliptic curve cryptosystem. *Journal of Supercomputing*, **2016**, 72, 3588-3600	2.5	8
116	RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks. *Journal of Parallel and Distributed Computing*, **2021**, 152, 1-10	4.4	8
115	A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks. *Security and Communication Networks*, **2019**, 2019, 1-13	1.9	8
114	An efficient blockchain-based batch verification scheme for vehicular ad hoc networks. *Transactions on Emerging Telecommunications Technologies*, **2019**,	1.9	8
113	PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications. *IEEE Systems Journal*, **2021**, 15, 4367-4378	4.3	8
112	SecureNLP: A System for Multi-Party Privacy-Preserving Natural Language Processing. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 3709-3721	8	7
111	A Blockchain-Based Proxy Re-Encryption With Equality Test for Vehicular Communication Systems. *IEEE Transactions on Network Science and Engineering*, **2020**, 1-1	4.9	7
110	A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing. *IEEE Access*, **2020**, 8, 28009-28020	3.5	7
109	Efficient and Provably Secure Distributed Signing Protocol for Mobile Devices in Wireless Networks. *IEEE Internet of Things Journal*, **2018**, 5, 5271-5280	10.7	7
108	Cryptanalysis of an Authenticated Key Agreement Protocol for Wireless Mobile Communications. *ETRI Journal*, **2012**, 34, 482-484	1.4	7
107	New large-universe multi-authority ciphertext-policy ABE scheme and its application in cloud storage systems. *Journal of High Speed Networks*, **2016**, 22, 153-167	0.4	7
106	Message-locked proof of ownership and retrievability with remote repairing in cloud. *Security and Communication Networks*, **2016**, 9, 3452-3466	1.9	7
105	An efficient chaos-based 2-party key agreement protocol with provable security. *International Journal of Communication Systems*, **2017**, 30, e3288	1.7	6
104	Efficient and Secure Ciphertext-Policy Attribute-Based Encryption Without Pairing for Cloud-Assisted Smart Grid. *IEEE Access*, **2020**, 8, 40704-40713	3.5	6

103	A novel proxy-oriented public auditing scheme for cloud-based medical cyber physical systems. *Journal of Information Security and Applications*, **2020**, 51, 102453	3.5	6
102	A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks. *Telecommunication Systems*, **2018**, 69, 431-445	2.3	6
101	Efficient ID-based multiproxy multisignature without bilinear maps in ROM. *Annales Des Telecommunications/Annals of Telecommunications*, **2013**, 68, 231-237	2	6
100	Cryptanalysis of a Dynamic ID-Based Remote User Authentication Scheme with Access Control for Multi-Server Environments. *IEICE Transactions on Information and Systems*, **2013**, E96.D, 138-140	0.6	6
99	Proofs of Ownership and Retrievability in Cloud Storage **2014**,		6
98	Cryptanalysis of a key agreement protocol based on chaotic Hash. *International Journal of Electronic Security and Digital Forensics*, **2013**, 5, 172	1	6
97	On the security of an authentication scheme for multi-server architecture. *International Journal of Electronic Security and Digital Forensics*, **2013**, 5, 288	1	6
96	Blockchain-based Privacy-preserving and Rewarding Private Data Sharing for IoT. *IEEE Internet of Things Journal*, **2022**, 1-1	10.7	6
95	A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. *Frontiers of Computer Science*, **2020**, 14, 1	2.2	6
94	Blockchain-based multi-party proof of assets with privacy preservation. *Information Sciences*, **2021**, 547, 609-621	7.7	6
93	CL-ME: Efficient Certificateless Matchmaking Encryption for Internet of Things. *IEEE Internet of Things Journal*, **2021**, 8, 15010-15023	10.7	6
92	Multi-Functional and Multi-Dimensional Secure Data Aggregation Schemes in WSNs. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	6
91	PAT: A precise reward scheme achieving anonymity and traceability for crowdcomputing in public clouds. *Future Generation Computer Systems*, **2018**, 79, 262-270	7.5	5
90	Cryptanalysis of a certificateless aggregate signature scheme with efficient verification. *Security and Communication Networks*, **2016**, n/a-n/a	1.9	5
89	An efficient password-based three-party authenticated multiple key exchange protocol for wireless mobile networks. *Journal of Supercomputing*, **2014**, 70, 224-235	2.5	5
88	An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network. *Journal of Information Security and Applications*, **2017**, 37, 112-121	3.5	5
87	Two-step single slope/SAR ADC with error correction for CMOS image sensor. *Scientific World Journal, The*, **2014**, 2014, 861278	2.2	5
86	Cryptanalysis of a Smartcard-Based User Authentication Scheme for Multi-Server Environments. *IEICE Transactions on Communications*, **2012**, E95.B, 3052-3054	0.5	5

85	Privacy-Enhancing Decentralized Anonymous Credential in Smart Grids. *Computer Standards and Interfaces*, **2021**, 75, 103505	3.5	5
84	Analysis and Improvement of a Certificateless Signature Scheme for Resource-Constrained Scenarios. *IEEE Communications Letters*, **2021**, 25, 1074-1078	3.8	5
83	White-Box Implementation of Shamir's Identity-Based Signature Scheme. *IEEE Systems Journal*, **2020**, 14, 1820-1829	4.3	5
82	An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. *Connection Science*, **2021**, 33, 1094-1115	2.8	5
81	PCNNCEC: Efficient and Privacy-Preserving Convolutional Neural Network Inference Based on Cloud-Edge-Client Collaboration. *IEEE Transactions on Network Science and Engineering*, **2022**, 1-1	4.9	5
80	Security Analysis of Two Password-Authenticated Multi-Key Exchange Protocols. *IEEE Access*, **2017**, 5, 8017-8024	3.5	4
79	Security analysis of a publicly verifiable data possession scheme for remote storage. *Journal of Supercomputing*, **2017**, 73, 4923-4930	2.5	4
78	Insecurity of a Pairing-Free Certificateless Ring Signcryption Scheme. *Wireless Personal Communications*, **2017**, 96, 5635-5641	1.9	4
77	A multi-objective optimization model based on immune algorithm in wireless mesh networks. *International Journal of Communication Systems*, **2016**, 29, 155-169	1.7	4
76	Enhanced authentication protocol for session initiation protocol using smart card. *International Journal of Electronic Security and Digital Forensics*, **2015**, 7, 330	1	4
75	Privacy Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey **2015**,		4
74	Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. *ACM Computing Surveys*, **2022**, 54, 1-36	13.4	4
73	Lightweight Collaborative Authentication With Key Protection for Smart Electronic Health Record System. *IEEE Sensors Journal*, **2020**, 20, 2181-2196	4	4
72	Multi-party key generation protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. *IET Information Security*, **2020**, 14, 724-732	1.4	4
71	Blockchain-based Data Sharing System for Sensing-as-a-Service in Smart Cities. *ACM Transactions on Internet Technology*, **2021**, 21, 1-21	3.8	4
70	Permissioned Blockchain-Based Anonymous and Traceable Aggregate Signature Scheme for Industrial Internet of Things. *IEEE Internet of Things Journal*, **2021**, 8, 8387-8398	10.7	4
69	Secure Storage Auditing With Efficient Key Updates for Cognitive Industrial IoT Environment. *IEEE Transactions on Industrial Informatics*, **2021**, 17, 4238-4247	11.9	4
68	An Efficient Privacy-Preserving Aggregation Scheme for Multi-dimensional Data in IoT. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	4

67	IEEE Access Special Section Editorial: Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies. *IEEE Access*, **2018**, 6, 72033-72036	3.5	4
66	. *IEEE Internet of Things Journal*, **2021**, 8, 14287-14298	10.7	4
65	Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks. *IEEE Systems Journal*, **2020**, 14, 5320-5328	4.3	3
64	Secure and Efficient Two-Factor Authentication Protocol Using RSA Signature for Multi-server Environments. *Lecture Notes in Computer Science*, **2018**, 595-605	0.9	3
63	A general compiler for password-authenticated group key exchange protocol in the standard model. *Discrete Applied Mathematics*, **2018**, 241, 78-86	1	3
62	A security enhanced mutual authentication scheme based on nonce and smart cards **2014**, 37, 1090-1095		3
61	A key distribution scheme using network coding for mobile ad hoc network. *Security and Communication Networks*, **2012**, 5, 59-67	1.9	3
60	On the Security of a Certificateless Proxy Signature Scheme with Message Recovery. *Mathematical Problems in Engineering*, **2013**, 2013, 1-4	1.1	3
59	Synchronized Provable Data Possession Based on Blockchain for Digital Twin. *IEEE Transactions on Information Forensics and Security*, **2022**, 17, 472-485	8	3
58	A Lattice-based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network. *IEEE Transactions on Vehicular Technology*, **2022**, 1-1	6.8	3
57	An Authenticated Key Agreement Protocol Using Isogenies Between Elliptic Curves. *International Journal of Computers, Communications and Control*, **2014**, 6, 258	3.6	3
56	An Efficient Data Aggregation Scheme with Local Differential Privacy in Smart Grid **2020**,		3
55	A Software/Hardware Co-Design of Crystals-Dilithium Signature Scheme. *ACM Transactions on Reconfigurable Technology and Systems*, **2021**, 14, 1-21	2.7	3
54	EPRT: An Efficient Privacy-Preserving Medical Service Recommendation and Trust Discovery Scheme for eHealth System. *ACM Transactions on Internet Technology*, **2021**, 21, 1-24	3.8	3
53	ESDR: an efficient and secure data repairing paradigm in cloud storage. *Security and Communication Networks*, **2016**, 9, 3646-3657	1.9	3
52	Isogeny-Based Cryptography: A Promising Post-Quantum Technique. *IT Professional*, **2019**, 21, 27-32	1.9	3
51	Semantics-Aware Privacy Risk Assessment Using Self-Learning Weight Assignment for Mobile Apps. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 15-29	3.9	3
50	An Efficient and Provably-Secure Certificateless Proxy-Signcryption Scheme for Electronic Prescription System. *Security and Communication Networks*, **2018**, 2018, 1-11	1.9	3

49	EBCPA: Efficient Blockchain-based Conditional Privacy-preserving Authentication for VANETs. *IEEE Transactions on Dependable and Secure Computing*, **2022**, 1-1	3.9	3
48	Efficient Certificateless Conditional Privacy-Preserving Authentication for VANETs. *IEEE Transactions on Vehicular Technology*, **2022**, 1-1	6.8	3
47	Insecurity of an Efficient Identity-Based Proxy Signature in the Standard Model. *Computer Journal*, **2015**, 58, 2507-2508	1.3	2
46	An Identity-Based Blind Signature Scheme Using Lattice with Provable Security. *Mathematical Problems in Engineering*, **2020**, 2020, 1-12	1.1	2
45	Charge-Depleting of the Batteries Makes Smartphones Recognizable **2017**,		2
44	Advances and Challenges in Convergent Communication Networks. *Wireless Personal Communications*, **2017**, 96, 4919-4927	1.9	2
43	Attribute-based fuzzy identity access control in multicloud computing environments. *Soft Computing*, **2018**, 22, 4071-4082	3.5	2
42	Balanced anonymity and traceability for outsourcing small-scale data linear aggregation in the smart grid. *IET Information Security*, **2017**, 11, 131-138	1.4	2
41	Weaknesses in a dynamic ID-based remote user authentication scheme for multi-server environment. *International Journal of Electronic Security and Digital Forensics*, **2012**, 4, 43	1	2
40	SAKE*: A Symmetric Authenticated Key Exchange Protocol with Perfect Forward Secrecy for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, **2022**, 1-1	11.9	2
39	Lattice-based undeniable signature scheme. *Annales Des Telecommunications/Annals of Telecommunications*,1	2	2
38	A Quantum Secure and Noninteractive Identity-Based Aggregate Signature Protocol From Lattices. *IEEE Systems Journal*, **2021**, 1-11	4.3	2
37	CaIAuth: Context-Aware Implicit Authentication When the Screen Is Awake. *IEEE Internet of Things Journal*, **2020**, 7, 11420-11430	10.7	2
36	Proxy Provable Data Possession with General Access Structure in Public Clouds. *Lecture Notes in Computer Science*, **2016**, 283-300	0.9	2
35	DELIA: Distributed Efficient Log Integrity Audit Based on Hierarchal Multi-Party State Channel. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	2
34	The Applications of Blockchain in Artificial Intelligence. *Security and Communication Networks*, **2021** , 2021, 1-16	1.9	2
33	XAuth: Efficient Privacy-preserving Cross-domain Authentication. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	2
32	ICAuth: Implicit and Continuous Authentication When the Screen Is Awake **2019**,		1

31	On the Security of a Key Agreement and Key Protection Scheme. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 3293-3294	8	1
30	An efficient and secure 3-factor user-authentication protocol for multiserver environment. *International Journal of Communication Systems*, **2018**, 31, e3734	1.7	1
29	Pairing-Free Identity-Based Encryption with Authorized Equality Test in Online Social Networks. *International Journal of Foundations of Computer Science*, **2019**, 30, 647-664	0.6	1
28	Cryptanalysis of an identity-based public auditing protocol for cloud storage. *Frontiers of Information Technology and Electronic Engineering*, **2017**, 18, 1972-1977	2.2	1
27	A Lightweight Mutual Authentication Scheme for User and Server in Cloud **2015**,		1
26	Provable Secure and Efficient Digital Rights Management Authentication Scheme Using Smart Card Based on Elliptic Curve Cryptography. *Mathematical Problems in Engineering*, **2015**, 2015, 1-16	1.1	1
25	Cryptanalysis of "An Improved Remote Password Authentication Scheme with Smartcard" **2013**,		1
24	A Redesigned Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	1
23	A Practical NIZK Argument for Confidential Transactions over Account-Model Blockchain. *Lecture Notes in Computer Science*, **2020**, 234-253	0.9	1
22	Oblivious Transfer Protocols Based on Group Factoring Problem. *Lecture Notes on Data Engineering and Communications Technologies*, **2017**, 885-892	0.4	1
21	Cryptanalysis of a certificateless aggregate signature scheme for mobile computation. *Applied Mathematics and Information Sciences*, **2013**, 7, 1383-1386	2.4	1
20	CsiIBS: A post-quantum identity-based signature scheme based on isogenies. *Journal of Information Security and Applications*, **2020**, 54, 102504	3.5	1
19	Privacy-preserving Data Aggregation against Malicious Data Mining Attack for IoT-enabled Smart Grid. *ACM Transactions on Sensor Networks*, **2021**, 17, 1-25	2.9	1
18	An Efficient Blind Signature Scheme Based on SM2 Signature Algorithm. *Lecture Notes in Computer Science*, **2021**, 368-384	0.9	1
17	An Efficient Privacy-Preserving Credit Score System Based on Noninteractive Zero-Knowledge Proof. *IEEE Systems Journal*, **2021**, 1-10	4.3	1
16	Efficient Distributed Decryption Scheme for IoT Gateway-based Applications. *ACM Transactions on Internet Technology*, **2021**, 21, 1-23	3.8	1
15	A General Architecture for Multiserver Authentication Key Agreement with Provable Security. *Security and Communication Networks*, **2018**, 2018, 1-9	1.9	1
14	An Efficient Identity-based Aggregate Signcryption Scheme with Blockchain for IoT-enabled Maritime Transportation System. *IEEE Transactions on Green Communications and Networking*, **2022**, 1-1	4	1

13	A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems. *Security and Communication Networks*, **2022**, 2022, 1-18	1.9	1
12	Hash-balanced binary tree□based public auditing in vehicular edge computing and networks. *International Journal of Communication Systems*, **2019**, e4134	1.7	0
11	Exploring Dynamic Task Loading in SGX-based Distributed Computing. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	0
10	A novel covert channel detection method in cloud based on XSRM and improved event association algorithm. *Security and Communication Networks*, **2016**, 9, 3543-3557	1.9	0
9	Efficient revocable ID-based encryption with cloud revocation server. *International Journal of Communication Systems*, **2018**, 31, e3386	1.7	0
8	The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. *IEEE Systems Journal*, **2022**, 1-12	4.3	0
7	An Adaptive Access Control Scheme based on Trust Degrees for Edge Computing. *Computer Standards and Interfaces*, **2022**, 103640	3.5	0
6	Security analysis of a user registration approach. *Journal of Supercomputing*, **2016**, 72, 900-903	2.5	
5	On Diophantine equation 3a 2 x 4 □By 2 = 1. *Annali Di Matematica Pura Ed Applicata*, **2010**, 189, 679-687	0.8	
4	Efficient and Secure Three-Factor User Authentication and Key Agreement Using Chaotic Maps. *Lecture Notes in Computer Science*, **2019**, 186-202	0.9	
3	DssP: Efficient Dual-Server Secret Sharing Protocol Based on Password Authentication for Cloud Storage Services. *IEEE Systems Journal*, **2021**, 1-11	4.3	
2	An Identity-Based Blind Signature and Its Application for Privacy Preservation in Bitcoin. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2021**, 10-24	0.2	
1	Spider-Inspired HCCapture: Beware That What You Are Writing on Mobile Devices Is Becoming Prey for Spiders.. *Frontiers in Bioengineering and Biotechnology*, **2022**, 10, 858961	5.8	