

De-biao He

List of Publications by Year in Descending Order

Source: <https://exaly.com/author-pdf/3566936/de-biao-he-publications-by-year.pdf>
Version: 2024-04-09

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.
The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

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

#	Paper	IF	Citations
264	Synchronized Provable Data Possession Based on Blockchain for Digital Twin. <i>IEEE Transactions on Information Forensics and Security</i> , 2022 , 17, 472-485	8	3
263	A Lattice-based Conditional Privacy-Preserving Authentication Protocol for the Vehicular Ad Hoc Network. <i>IEEE Transactions on Vehicular Technology</i> , 2022 , 1-1	6.8	3
262	SAKE*: A Symmetric Authenticated Key Exchange Protocol with Perfect Forward Secrecy for Industrial Internet of Things. <i>IEEE Transactions on Industrial Informatics</i> , 2022 , 1-1	11.9	2
261	Blockchain-based Privacy-preserving and Rewarding Private Data Sharing for IoT. <i>IEEE Internet of Things Journal</i> , 2022 , 1-1	10.7	6
260	Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. <i>ACM Computing Surveys</i> , 2022 , 54, 1-36	13.4	4
259	Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. <i>Science China Information Sciences</i> , 2022 , 65, 1	3.4	25
258	The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. <i>IEEE Systems Journal</i> , 2022 , 1-12	4.3	0
257	EBCPA: Efficient Blockchain-based Conditional Privacy-preserving Authentication for VANETs. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2022 , 1-1	3.9	3
256	An Efficient Identity-based Aggregate Signcryption Scheme with Blockchain for IoT-enabled Maritime Transportation System. <i>IEEE Transactions on Green Communications and Networking</i> , 2022 , 1-1	4	1
255	A Blockchain-Based User Authentication Scheme with Access Control for Telehealth Systems. <i>Security and Communication Networks</i> , 2022 , 2022, 1-18	1.9	1
254	An Adaptive Access Control Scheme based on Trust Degrees for Edge Computing. <i>Computer Standards and Interfaces</i> , 2022 , 103640	3.5	0
253	Spider-Inspired HCCapture: Beware That What You Are Writing on Mobile Devices Is Becoming Prey for Spiders.. <i>Frontiers in Bioengineering and Biotechnology</i> , 2022 , 10, 858961	5.8	
252	Efficient Certificateless Conditional Privacy-Preserving Authentication for VANETs. <i>IEEE Transactions on Vehicular Technology</i> , 2022 , 1-1	6.8	3
251	PCNNCEC: Efficient and Privacy-Preserving Convolutional Neural Network Inference Based on Cloud-Edge-Client Collaboration. <i>IEEE Transactions on Network Science and Engineering</i> , 2022 , 1-1	4.9	5
250	A Quantum Secure and Noninteractive Identity-Based Aggregate Signature Protocol From Lattices. <i>IEEE Systems Journal</i> , 2021 , 1-11	4.3	2
249	A Redesigned Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	1
248	Exploring Dynamic Task Loading in SGX-based Distributed Computing. <i>IEEE Transactions on Services Computing</i> , 2021 , 1-1	4.8	0

247	DssP: Efficient Dual-Server Secret Sharing Protocol Based on Password Authentication for Cloud Storage Services. <i>IEEE Systems Journal</i> , 2021 , 1-11	4.3	
246	Blockchain-based Data Sharing System for Sensing-as-a-Service in Smart Cities. <i>ACM Transactions on Internet Technology</i> , 2021 , 21, 1-21	3.8	4
245	Privacy-Enhancing Decentralized Anonymous Credential in Smart Grids. <i>Computer Standards and Interfaces</i> , 2021 , 75, 103505	3.5	5
244	Analysis and Improvement of a Certificateless Signature Scheme for Resource-Constrained Scenarios. <i>IEEE Communications Letters</i> , 2021 , 25, 1074-1078	3.8	5
243	Permissioned Blockchain-Based Anonymous and Traceable Aggregate Signature Scheme for Industrial Internet of Things. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 8387-8398	10.7	4
242	Privacy-preserving Data Aggregation against Malicious Data Mining Attack for IoT-enabled Smart Grid. <i>ACM Transactions on Sensor Networks</i> , 2021 , 17, 1-25	2.9	1
241	A Software/Hardware Co-Design of Crystals-Dilithium Signature Scheme. <i>ACM Transactions on Reconfigurable Technology and Systems</i> , 2021 , 14, 1-21	2.7	3
240	The Application of the Blockchain Technology in Voting Systems. <i>ACM Computing Surveys</i> , 2021 , 54, 1-28	13.4	9
239	RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks. <i>Journal of Parallel and Distributed Computing</i> , 2021 , 152, 1-10	4.4	8
238	EPRT: An Efficient Privacy-Preserving Medical Service Recommendation and Trust Discovery Scheme for eHealth System. <i>ACM Transactions on Internet Technology</i> , 2021 , 21, 1-24	3.8	3
237	An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 18, 641-651	3.9	22
236	Secure Storage Auditing With Efficient Key Updates for Cognitive Industrial IoT Environment. <i>IEEE Transactions on Industrial Informatics</i> , 2021 , 17, 4238-4247	11.9	4
235	An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 458-473	10.7	24
234	A Survey of Blockchain Applications in the Energy Sector. <i>IEEE Systems Journal</i> , 2021 , 15, 3370-3381	4.3	28
233	Semantics-Aware Privacy Risk Assessment Using Self-Learning Weight Assignment for Mobile Apps. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 18, 15-29	3.9	3
232	. <i>IEEE Transactions on Intelligent Transportation Systems</i> , 2021 , 22, 3939-3951	6.1	18
231	PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications. <i>IEEE Systems Journal</i> , 2021 , 15, 4367-4378	4.3	8
230	Blockchain-based multi-party proof of assets with privacy preservation. <i>Information Sciences</i> , 2021 , 547, 609-621	7.7	6

229	Efficient Identity-Based Distributed Decryption Scheme for Electronic Personal Health Record Sharing System. <i>IEEE Journal on Selected Areas in Communications</i> , 2021 , 39, 384-395	14.2	9
228	Dynamic Group-Oriented Provable Data Possession in the Cloud. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 1-1	3.9	13
227	An Efficient Blind Signature Scheme Based on SM2 Signature Algorithm. <i>Lecture Notes in Computer Science</i> , 2021 , 368-384	0.9	1
226	OBFP: Optimized Blockchain-Based Fair Payment for Outsourcing Computations in Cloud Computing. <i>IEEE Transactions on Information Forensics and Security</i> , 2021 , 16, 3241-3253	8	11
225	An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. <i>Connection Science</i> , 2021 , 33, 1094-1115	2.8	5
224	An Efficient Privacy-Preserving Credit Score System Based on Noninteractive Zero-Knowledge Proof. <i>IEEE Systems Journal</i> , 2021 , 1-10	4.3	1
223	An Efficient Privacy-Preserving Aggregation Scheme for Multi-dimensional Data in IoT. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	4
222	An Identity-Based Blind Signature and Its Application for Privacy Preservation in Bitcoin. <i>Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering</i> , 2021 , 10-24	0.2	
221	Blockchain-Based Secure and Lightweight Authentication for Internet of Things. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	9
220	DELIA: Distributed Efficient Log Integrity Audit Based on Hierarchical Multi-Party State Channel. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 1-1	3.9	2
219	Efficient Distributed Decryption Scheme for IoT Gateway-based Applications. <i>ACM Transactions on Internet Technology</i> , 2021 , 21, 1-23	3.8	1
218	. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 14287-14298	10.7	4
217	The Applications of Blockchain in Artificial Intelligence. <i>Security and Communication Networks</i> , 2021 , 2021, 1-16	1.9	2
216	CL-ME: Efficient Certificateless Matchmaking Encryption for Internet of Things. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 15010-15023	10.7	6
215	Multi-Functional and Multi-Dimensional Secure Data Aggregation Schemes in WSNs. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	6
214	XAuth: Efficient Privacy-preserving Cross-domain Authentication. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 1-1	3.9	2
213	SecureNLP: A System for Multi-Party Privacy-Preserving Natural Language Processing. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 3709-3721	8	7
212	Blockchain-based identity management systems: A review. <i>Journal of Network and Computer Applications</i> , 2020 , 166, 102731	7.9	53

211	A Blockchain-Based Proxy Re-Encryption With Equality Test for Vehicular Communication Systems. <i>IEEE Transactions on Network Science and Engineering</i> , 2020 , 1-1	4.9	7
210	Efficient NTRU Lattice-Based Certificateless Signature Scheme for Medical Cyber-Physical Systems. <i>Journal of Medical Systems</i> , 2020 , 44, 92	5.1	11
209	Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks. <i>IEEE Systems Journal</i> , 2020 , 14, 5320-5328	4.3	3
208	White-Box Implementation of the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. <i>IEICE Transactions on Information and Systems</i> , 2020 , E103.D, 188-195	0.6	10
207	Efficient and Secure Ciphertext-Policy Attribute-Based Encryption Without Pairing for Cloud-Assisted Smart Grid. <i>IEEE Access</i> , 2020 , 8, 40704-40713	3.5	6
206	An Identity-Based Blind Signature Scheme Using Lattice with Provable Security. <i>Mathematical Problems in Engineering</i> , 2020 , 2020, 1-12	1.1	2
205	Human-in-the-Loop-Aided Privacy-Preserving Scheme for Smart Healthcare. <i>IEEE Transactions on Emerging Topics in Computational Intelligence</i> , 2020 , 1-10	4.1	13
204	BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks. <i>IEEE Transactions on Intelligent Transportation Systems</i> , 2020 , 1-13	6.1	40
203	SecBCS: a secure and privacy-preserving blockchain-based crowdsourcing system. <i>Science China Information Sciences</i> , 2020 , 63, 1	3.4	20
202	Efficient Certificateless Aggregate Signature Scheme for Performing Secure Routing in VANETs. <i>Security and Communication Networks</i> , 2020 , 2020, 1-12	1.9	12
201	A lightweight authentication and key agreement scheme for Internet of Drones. <i>Computer Communications</i> , 2020 , 154, 455-464	5.1	57
200	A novel proxy-oriented public auditing scheme for cloud-based medical cyber physical systems. <i>Journal of Information Security and Applications</i> , 2020 , 51, 102453	3.5	6
199	An efficient and provable certificate-based proxy signature scheme for IIoT environment. <i>Information Sciences</i> , 2020 , 518, 142-156	7.7	14
198	A Parallel and Forward Private Searchable Public-Key Encryption for Cloud-Based Data Sharing. <i>IEEE Access</i> , 2020 , 8, 28009-28020	3.5	7
197	DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 2440-2452	8	46
196	On the Security of a Key Agreement and Key Protection Scheme. <i>IEEE Transactions on Information Forensics and Security</i> , 2020 , 15, 3293-3294	8	1
195	An Efficient Data Aggregation Scheme with Local Differential Privacy in Smart Grid 2020 ,		3
194	A Practical NIZK Argument for Confidential Transactions over Account-Model Blockchain. <i>Lecture Notes in Computer Science</i> , 2020 , 234-253	0.9	1

193	. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 6056-6068	10.7	17
192	BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks. <i>IEEE Transactions on Industrial Informatics</i> , 2020 , 16, 4146-4155	11.9	88
191	Lightweight Collaborative Authentication With Key Protection for Smart Electronic Health Record System. <i>IEEE Sensors Journal</i> , 2020 , 20, 2181-2196	4	4
190	A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. <i>Frontiers of Computer Science</i> , 2020 , 14, 1	2.2	6
189	Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare. <i>Journal of Information Security and Applications</i> , 2020 , 50, 102429	3.5	10
188	A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks. <i>IEEE Transactions on Vehicular Technology</i> , 2020 , 69, 5813-5825	6.8	27
187	Multi-party key generation protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. <i>IET Information Security</i> , 2020 , 14, 724-732	1.4	4
186	CalAuth: Context-Aware Implicit Authentication When the Screen Is Awake. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 11420-11430	10.7	2
185	Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. <i>Computers and Security</i> , 2020 , 97, 101966	4.9	92
184	CsIBS: A post-quantum identity-based signature scheme based on isogenies. <i>Journal of Information Security and Applications</i> , 2020 , 54, 102504	3.5	1
183	Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme. <i>IET Information Security</i> , 2020 , 14, 443-451	1.4	15
182	Algebraic Signatures-Based Data Integrity Auditing for Efficient Data Dynamics in Cloud Computing. <i>IEEE Transactions on Sustainable Computing</i> , 2020 , 5, 161-173	3.5	11
181	Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography. <i>Future Generation Computer Systems</i> , 2020 , 107, 854-862	7.5	30
180	VOD-ADAC: Anonymous Distributed Fine-Grained Access Control Protocol with Verifiable Outsourced Decryption in Public Cloud. <i>IEEE Transactions on Services Computing</i> , 2020 , 13, 572-583	4.8	24
179	Blockchain-based system for secure outsourcing of bilinear pairings. <i>Information Sciences</i> , 2020 , 527, 590-601	7.7	32
178	A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing. <i>IEEE Systems Journal</i> , 2020 , 14, 560-571	4.3	64
177	White-Box Implementation of Shamir's Identity-Based Signature Scheme. <i>IEEE Systems Journal</i> , 2020 , 14, 1820-1829	4.3	5
176	Blockchain-Based Anonymous Reporting Scheme With Anonymous Rewarding. <i>IEEE Transactions on Engineering Management</i> , 2020 , 67, 1514-1524	2.6	9

175	Secure and Efficient Two-Party Signing Protocol for the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 17, 1124-1132	3.9	25
174	HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 818-829	10.7	65
173	CB-PS: An Efficient Short-Certificate-Based Proxy Signature Scheme for UAVs. <i>IEEE Systems Journal</i> , 2020 , 14, 621-632	4.3	14
172	Blockchain-Based Anonymous Authentication With Key Management for Smart Grid Edge Computing Infrastructure. <i>IEEE Transactions on Industrial Informatics</i> , 2020 , 16, 1984-1992	11.9	86
171	ICAuth: Implicit and Continuous Authentication When the Screen Is Awake 2019 ,		1
170	Anonymous and Efficient Message Authentication Scheme for Smart Grid. <i>Security and Communication Networks</i> , 2019 , 2019, 1-12	1.9	15
169	. <i>IEEE Consumer Electronics Magazine</i> , 2019 , 8, 45-49	3.2	27
168	An Efficient and Provably Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. <i>IEEE Internet of Things Journal</i> , 2019 , 6, 8065-8075	10.7	63
167	Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices. <i>IEEE Systems Journal</i> , 2019 , 13, 2775-2785	4.3	25
166	Authenticated key agreement scheme for fog-driven IoT healthcare system. <i>Wireless Networks</i> , 2019 , 25, 4737-4750	2.5	86
165	Secure Key Agreement and Key Protection for Mobile Device User Authentication. <i>IEEE Transactions on Information Forensics and Security</i> , 2019 , 14, 319-330	8	79
164	Privacy-preserving incentive and rewarding scheme for crowd computing in social media. <i>Information Sciences</i> , 2019 , 470, 15-27	7.7	10
163	Hash-balanced binary treeBased public auditing in vehicular edge computing and networks. <i>International Journal of Communication Systems</i> , 2019 , e4134	1.7	0
162	Pairing-Free Identity-Based Encryption with Authorized Equality Test in Online Social Networks. <i>International Journal of Foundations of Computer Science</i> , 2019 , 30, 647-664	0.6	1
161	Lightweight Searchable Public-key Encryption with Forward Privacy over IIoT Outsourced Data. <i>IEEE Transactions on Emerging Topics in Computing</i> , 2019 , 1-1	4.1	18
160	Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network. <i>IEEE Transactions on Vehicular Technology</i> , 2019 , 68, 11309-11322	6.8	53
159	Dual-Server Public-Key Authenticated Encryption With Keyword Search. <i>IEEE Transactions on Cloud Computing</i> , 2019 , 1-1	3.3	10
158	Blockchain-Based Private Provable Data Possession. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2019 , 1-1	3.9	13

157	Efficient and Secure Three-Factor User Authentication and Key Agreement Using Chaotic Maps. <i>Lecture Notes in Computer Science</i> , 2019 , 186-202	0.9	
156	Blockchain in healthcare applications: Research challenges and opportunities. <i>Journal of Network and Computer Applications</i> , 2019 , 135, 62-75	7.9	271
155	A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks. <i>Security and Communication Networks</i> , 2019 , 2019, 1-13	1.9	8
154	An efficient blockchain-based batch verification scheme for vehicular ad hoc networks. <i>Transactions on Emerging Telecommunications Technologies</i> , 2019 ,	1.9	8
153	Isogeny-Based Cryptography: A Promising Post-Quantum Technique. <i>IT Professional</i> , 2019 , 21, 27-32	1.9	3
152	BBARS: Blockchain-Based Anonymous Rewarding Scheme for V2G Networks. <i>IEEE Internet of Things Journal</i> , 2019 , 6, 3676-3687	10.7	34
151	A survey on privacy protection in blockchain system. <i>Journal of Network and Computer Applications</i> , 2019 , 126, 45-58	7.9	302
150	. <i>IEEE Transactions on Services Computing</i> , 2019 , 1-1	4.8	24
149	Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things. <i>Annales Des Telecommunications/Annals of Telecommunications</i> , 2019 , 74, 423-434	2	24
148	PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management. <i>IEEE Access</i> , 2019 , 7, 6117-6128	3.5	20
147	Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2019 , 16, 996-1010	3.9	97
146	Improved secure fuzzy auditing protocol for cloud data storage. <i>Soft Computing</i> , 2019 , 23, 3411-3422	3.5	16
145	Incentive and Unconditionally Anonymous Identity-Based Public Provable Data Possession. <i>IEEE Transactions on Services Computing</i> , 2019 , 12, 824-835	4.8	49
144	Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks. <i>IEEE Systems Journal</i> , 2018 , 12, 64-73	4.3	147
143	Secure and Efficient Two-Factor Authentication Protocol Using RSA Signature for Multi-server Environments. <i>Lecture Notes in Computer Science</i> , 2018 , 595-605	0.9	3
142	Security and Privacy for the Internet of Drones: Challenges and Solutions. <i>IEEE Communications Magazine</i> , 2018 , 56, 64-69	9.1	159
141	Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. <i>IEEE Transactions on Industrial Informatics</i> , 2018 , 14, 3618-3627	11.9	102
140	Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems. <i>IEEE Transactions on Industrial Informatics</i> , 2018 , 14, 1232-1241	11.9	50

139	Signature-based three-factor authenticated key exchange for internet of things applications. <i>Multimedia Tools and Applications</i> , 2018 , 77, 18355-18382	2.5	12
138	An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment. <i>Ad Hoc Networks</i> , 2018 , 71, 78-87	4.8	46
137	A secure enhanced privacy-preserving key agreement protocol for wireless mobile networks. <i>Telecommunication Systems</i> , 2018 , 69, 431-445	2.3	6
136	Blind Filtering at Third Parties: An Efficient Privacy-Preserving Framework for Location-Based Services. <i>IEEE Transactions on Mobile Computing</i> , 2018 , 17, 2524-2535	4.6	46
135	. <i>IEEE Systems Journal</i> , 2018 , 12, 916-925	4.3	80
134	A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2018 , 15, 633-645	3.9	83
133	A general compiler for password-authenticated group key exchange protocol in the standard model. <i>Discrete Applied Mathematics</i> , 2018 , 241, 78-86	1	3
132	Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. <i>IEEE Systems Journal</i> , 2018 , 12, 1621-1631	4.3	97
131	PAT: A precise reward scheme achieving anonymity and traceability for crowdcomputing in public clouds. <i>Future Generation Computer Systems</i> , 2018 , 79, 262-270	7.5	5
130	Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. <i>IEEE Transactions on Industrial Informatics</i> , 2018 , 14, 759-767	11.9	144
129	Attribute-based fuzzy identity access control in multicloud computing environments. <i>Soft Computing</i> , 2018 , 22, 4071-4082	3.5	2
128	Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption. <i>Soft Computing</i> , 2018 , 22, 707-714	3.5	20
127	Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps. <i>Soft Computing</i> , 2018 , 22, 2267-2274	3.5	18
126	Certificateless searchable public key encryption scheme for mobile healthcare system. <i>Computers and Electrical Engineering</i> , 2018 , 65, 413-424	4.3	41
125	Efficient and secure searchable encryption protocol for cloud-based Internet of Things. <i>Journal of Parallel and Distributed Computing</i> , 2018 , 111, 152-161	4.4	32
124	Taxonomy and analysis of security protocols for Internet of Things. <i>Future Generation Computer Systems</i> , 2018 , 89, 110-125	7.5	94
123	An efficient and secure 3-factor user-authentication protocol for multiserver environment. <i>International Journal of Communication Systems</i> , 2018 , 31, e3734	1.7	1
122	Compact Hardware Implementation of a SHA-3 Core for Wireless Body Sensor Networks. <i>IEEE Access</i> , 2018 , 6, 40128-40136	3.5	12

121	New Certificateless Aggregate Signature Scheme for Healthcare Multimedia Social Network on Cloud Environment. <i>Security and Communication Networks</i> , 2018 , 2018, 1-13	1.9	25
120	Efficient and Provably Secure Distributed Signing Protocol for Mobile Devices in Wireless Networks. <i>IEEE Internet of Things Journal</i> , 2018 , 5, 5271-5280	10.7	7
119	Privacy-preserving auditing scheme for shared data in public clouds. <i>Journal of Supercomputing</i> , 2018 , 74, 6156-6183	2.5	10
118	. <i>IEEE Transactions on Sustainable Computing</i> , 2018 , 3, 44-55	3.5	29
117	Efficient revocable ID-based encryption with cloud revocation server. <i>International Journal of Communication Systems</i> , 2018 , 31, e3386	1.7	0
116	Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. <i>Future Generation Computer Systems</i> , 2018 , 84, 239-251	7.5	57
115	BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT. <i>Wireless Communications and Mobile Computing</i> , 2018 , 2018, 1-9	1.9	38
114	A General Architecture for Multiserver Authentication Key Agreement with Provable Security. <i>Security and Communication Networks</i> , 2018 , 2018, 1-9	1.9	1
113	IEEE Access Special Section Editorial: Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies. <i>IEEE Access</i> , 2018 , 6, 72033-72036	3.5	4
112	An Efficient and Provably-Secure Certificateless Proxy-Signcryption Scheme for Electronic Prescription System. <i>Security and Communication Networks</i> , 2018 , 2018, 1-11	1.9	3
111	A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems. <i>IEEE Access</i> , 2018 , 6, 28203-28212	3.5	44
110	BSeln: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. <i>Journal of Network and Computer Applications</i> , 2018 , 116, 42-52	7.9	212
109	An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. <i>Soft Computing</i> , 2018 , 22, 7685-7696	3.5	19
108	Anonymous Authentication for Wireless Body Area Networks With Provable Security. <i>IEEE Systems Journal</i> , 2017 , 11, 2590-2601	4.3	248
107	Succinct multi-authority attribute-based access control for circuits with authenticated outsourcing. <i>Soft Computing</i> , 2017 , 21, 5265-5279	3.5	8
106	Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices. <i>Soft Computing</i> , 2017 , 21, 6801-6810	3.5	30
105	An efficient chaos-based 2-party key agreement protocol with provable security. <i>International Journal of Communication Systems</i> , 2017 , 30, e3288	1.7	6
104	Efficient Revocable ID-Based Signature With Cloud Revocation Server. <i>IEEE Access</i> , 2017 , 5, 2945-2954	3.5	19

103	Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. <i>IEEE Access</i> , 2017 , 5, 3376-3392	3.5	198
102	Security Analysis of Two Password-Authenticated Multi-Key Exchange Protocols. <i>IEEE Access</i> , 2017 , 5, 8017-8024	3.5	4
101	Security analysis of a publicly verifiable data possession scheme for remote storage. <i>Journal of Supercomputing</i> , 2017 , 73, 4923-4930	2.5	4
100	A secure and efficient public auditing scheme using RSA algorithm for cloud storage. <i>Journal of Supercomputing</i> , 2017 , 73, 5285-5309	2.5	11
99	Insecurity of a Pairing-Free Certificateless Ring Signcryption Scheme. <i>Wireless Personal Communications</i> , 2017 , 96, 5635-5641	1.9	4
98	A secure and efficient identity-based mutual authentication scheme with smart card using elliptic curve cryptography. <i>International Journal of Communication Systems</i> , 2017 , 30, e3333	1.7	11
97	Efficient and secure identity-based encryption scheme with equality test in cloud computing. <i>Future Generation Computer Systems</i> , 2017 , 73, 22-31	7.5	63
96	Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. <i>Computer Networks</i> , 2017 , 128, 154-163	5.4	18
95	Lightweight Data Aggregation Scheme against Internal Attackers in Smart Grid Using Elliptic Curve Cryptography. <i>Wireless Communications and Mobile Computing</i> , 2017 , 2017, 1-11	1.9	24
94	Charge-Depleting of the Batteries Makes Smartphones Recognizable 2017 ,		2
93	Advances and Challenges in Convergent Communication Networks. <i>Wireless Personal Communications</i> , 2017 , 96, 4919-4927	1.9	2
92	An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network. <i>Journal of Information Security and Applications</i> , 2017 , 37, 112-121	3.5	5
91	Secure public data auditing scheme for cloud storage in smart city. <i>Personal and Ubiquitous Computing</i> , 2017 , 21, 949-962	2.1	12
90	Privacy-preserving certificateless provable data possession scheme for big data storage on cloud. <i>Applied Mathematics and Computation</i> , 2017 , 314, 31-43	2.7	38
89	Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries. <i>IEEE Transactions on Smart Grid</i> , 2017 , 8, 2411-2419	10.7	124
88	Efficient Hierarchical Identity-Based Signature With Batch Verification for Automatic Dependent Surveillance-Broadcast System. <i>IEEE Transactions on Information Forensics and Security</i> , 2017 , 12, 454-464	8	39
87	A secure data backup scheme using multi-factor authentication. <i>IET Information Security</i> , 2017 , 11, 250-254	5.5	17
86	Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation. <i>Science China Information Sciences</i> , 2017 , 60, 1	3.4	32

85	A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. <i>International Journal of Network Management</i> , 2017 , 27, e1937	1.8	22
84	Balanced anonymity and traceability for outsourcing small-scale data linear aggregation in the smart grid. <i>IET Information Security</i> , 2017 , 11, 131-138	1.4	2
83	Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage. <i>Information Sciences</i> , 2017 , 375, 48-53	7.7	27
82	Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing. <i>Soft Computing</i> , 2017 , 21, 7325-7335	3.5	37
81	Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks. <i>IEEE Transactions on Mobile Computing</i> , 2017 , 16, 1530-1543	4.6	40
80	Cryptanalysis of an identity-based public auditing protocol for cloud storage. <i>Frontiers of Information Technology and Electronic Engineering</i> , 2017 , 18, 1972-1977	2.2	1
79	Oblivious Transfer Protocols Based on Group Factoring Problem. <i>Lecture Notes on Data Engineering and Communications Technologies</i> , 2017 , 885-892	0.4	1
78	Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 2052-2064	8	117
77	Cryptanalysis of a certificateless aggregate signature scheme with efficient verification. <i>Security and Communication Networks</i> , 2016 , n/a-n/a	1.9	5
76	A multi-objective optimization model based on immune algorithm in wireless mesh networks. <i>International Journal of Communication Systems</i> , 2016 , 29, 155-169	1.7	4
75	Privacy-preserving data aggregation scheme against internal attackers in smart grids. <i>Wireless Networks</i> , 2016 , 22, 491-502	2.5	85
74	Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 1165-1176	8	115
73	A security-enhanced authentication with key agreement scheme for wireless mobile communications using elliptic curve cryptosystem. <i>Journal of Supercomputing</i> , 2016 , 72, 3588-3600	2.5	8
72	A privacy preserving three-factor authentication protocol for e-Health clouds. <i>Journal of Supercomputing</i> , 2016 , 72, 3826-3849	2.5	135
71	Security analysis of a user registration approach. <i>Journal of Supercomputing</i> , 2016 , 72, 900-903	2.5	
70	New large-universe multi-authority ciphertext-policy ABE scheme and its application in cloud storage systems. <i>Journal of High Speed Networks</i> , 2016 , 22, 153-167	0.4	7
69	One-to-many authentication for access control in mobile pay-TV systems. <i>Science China Information Sciences</i> , 2016 , 59, 1	3.4	55
68	DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments. <i>IEEE Transactions on Computers</i> , 2016 , 65, 3631-3645	2.5	49

67	Proxy Provable Data Possession with General Access Structure in Public Clouds. <i>Lecture Notes in Computer Science</i> , 2016 , 283-300	0.9	2
66	A novel covert channel detection method in cloud based on XSRM and improved event association algorithm. <i>Security and Communication Networks</i> , 2016 , 9, 3543-3557	1.9	0
65	ESDR: an efficient and secure data repairing paradigm in cloud storage. <i>Security and Communication Networks</i> , 2016 , 9, 3646-3657	1.9	3
64	Message-locked proof of ownership and retrievability with remote repairing in cloud. <i>Security and Communication Networks</i> , 2016 , 9, 3452-3466	1.9	7
63	Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. <i>IET Communications</i> , 2016 , 10, 1795-1802	1.3	80
62	New biometrics-based authentication scheme for multi-server environment in critical systems. <i>Journal of Ambient Intelligence and Humanized Computing</i> , 2015 , 6, 825-834	3.7	57
61	Efficient provably secure password-based explicit authenticated key agreement. <i>Pervasive and Mobile Computing</i> , 2015 , 24, 50-60	3.5	12
60	A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. <i>Information Sciences</i> , 2015 , 321, 263-277	7.7	177
59	Secure pseudonym-based near field communication protocol for the consumer internet of things. <i>IEEE Transactions on Consumer Electronics</i> , 2015 , 61, 56-62	4.8	23
58	An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. <i>IEEE Transactions on Information Forensics and Security</i> , 2015 , 10, 2681-2691	8	465
57	Dominating Set and Network Coding-Based Routing in Wireless Mesh Networks. <i>IEEE Transactions on Parallel and Distributed Systems</i> , 2015 , 26, 423-433	3.7	38
56	Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. <i>Multimedia Systems</i> , 2015 , 21, 49-60	2.2	211
55	Robust Biometrics-Based Authentication Scheme for Multiserver Environment. <i>IEEE Systems Journal</i> , 2015 , 9, 816-823	4.3	286
54	Insecurity of an Efficient Identity-Based Proxy Signature in the Standard Model. <i>Computer Journal</i> , 2015 , 58, 2507-2508	1.3	2
53	An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. <i>IEEE Internet of Things Journal</i> , 2015 , 2, 72-83	10.7	178
52	Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2015 , 12, 428-442	3.9	276
51	Enhanced authentication protocol for session initiation protocol using smart card. <i>International Journal of Electronic Security and Digital Forensics</i> , 2015 , 7, 330	1	4
50	Privacy Preserving Search Schemes over Encrypted Cloud Data: A Comparative Survey 2015 ,		4

49	A Lightweight Mutual Authentication Scheme for User and Server in Cloud 2015 ,		1
48	Provable Secure and Efficient Digital Rights Management Authentication Scheme Using Smart Card Based on Elliptic Curve Cryptography. <i>Mathematical Problems in Engineering</i> , 2015 , 2015, 1-16	1.1	1
47	An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography. <i>Wireless Personal Communications</i> , 2015 , 85, 225-240	1.9	25
46	A new handover authentication protocol based on bilinear pairing functions for wireless networks. <i>International Journal of Ad Hoc and Ubiquitous Computing</i> , 2015 , 18, 67	0.7	25
45	Authentication protocol for an ambient assisted living system 2015 , 53, 71-77		159
44	Enhanced three-factor security protocol for consumer USB mass storage devices. <i>IEEE Transactions on Consumer Electronics</i> , 2014 , 60, 30-37	4.8	135
43	An efficient password-based three-party authenticated multiple key exchange protocol for wireless mobile networks. <i>Journal of Supercomputing</i> , 2014 , 70, 224-235	2.5	5
42	Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. <i>Journal of Medical Systems</i> , 2014 , 38, 116	5.1	71
41	Insecurity of an efficient certificateless aggregate signature with constant pairing computations. <i>Information Sciences</i> , 2014 , 268, 458-462	7.7	52
40	Two-step single slope/SAR ADC with error correction for CMOS image sensor. <i>Scientific World Journal, The</i> , 2014 , 2014, 861278	2.2	5
39	Reattack of a certificateless aggregate signature scheme with constant pairing computations. <i>Scientific World Journal, The</i> , 2014 , 2014, 343715	2.2	21
38	Proofs of Ownership and Retrieval in Cloud Storage 2014 ,		6
37	A security enhanced mutual authentication scheme based on nonce and smart cards 2014 , 37, 1090-1095		3
36	Cryptanalysis and Improvement of an Anonymous Authentication Protocol for Wireless Access Networks. <i>Wireless Personal Communications</i> , 2014 , 74, 229-243	1.9	51
35	An Authenticated Key Agreement Protocol Using Isogenies Between Elliptic Curves. <i>International Journal of Computers, Communications and Control</i> , 2014 , 6, 258	3.6	3
34	Security Flaws in a Smart Card Based Authentication Scheme for Multi-server Environment. <i>Wireless Personal Communications</i> , 2013 , 70, 323-329	1.9	44
33	Efficient ID-based multiproxy multisignature without bilinear maps in ROM. <i>Annales Des Telecommunications/Annals of Telecommunications</i> , 2013 , 68, 231-237	2	6
32	Cryptanalysis of a Dynamic ID-Based Remote User Authentication Scheme with Access Control for Multi-Server Environments. <i>IEICE Transactions on Information and Systems</i> , 2013 , E96.D, 138-140	0.6	6

31	An Id-Based Three-Party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography For Mobile-Commerce Environments. <i>Arabian Journal for Science and Engineering</i> , 2013 , 38, 2055-2061		16
30	An efficient certificateless proxy signature scheme without pairing. <i>Mathematical and Computer Modelling</i> , 2013 , 57, 2510-2518		31
29	Anonymous two-factor authentication for consumer roaming service in global mobility networks. <i>IEEE Transactions on Consumer Electronics</i> , 2013 , 59, 811-817	4.8	62
28	New certificateless short signature scheme. <i>IET Information Security</i> , 2013 , 7, 113-117	1.4	43
27	On the Security of a Certificateless Proxy Signature Scheme with Message Recovery. <i>Mathematical Problems in Engineering</i> , 2013 , 2013, 1-4	1.1	3
26	Cryptanalysis of "An Improved Remote Password Authentication Scheme with Smartcard" 2013 ,		1
25	Cryptanalysis of a key agreement protocol based on chaotic Hash. <i>International Journal of Electronic Security and Digital Forensics</i> , 2013 , 5, 172	1	6
24	On the security of an authentication scheme for multi-server architecture. <i>International Journal of Electronic Security and Digital Forensics</i> , 2013 , 5, 288	1	6
23	Cryptanalysis and Improvement of a Password-Based Remote User Authentication Scheme without Smart Cards. <i>Information Technology and Control</i> , 2013 , 42,	1.3	11
22	Cryptanalysis of a certificateless aggregate signature scheme for mobile computation. <i>Applied Mathematics and Information Sciences</i> , 2013 , 7, 1383-1386	2.4	1
21	An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. <i>Information Fusion</i> , 2012 , 13, 223-230	16.7	142
20	Note on Design of improved password authentication and update scheme based on elliptic curve cryptography. <i>Mathematical and Computer Modelling</i> , 2012 , 55, 1661-1664		15
19	Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol. <i>Information Sciences</i> , 2012 , 215, 83-96	7.7	23
18	An efficient certificateless two-party authenticated key agreement protocol. <i>Computers and Mathematics With Applications</i> , 2012 , 64, 1914-1926	2.7	48
17	Cryptanalysis of an Authenticated Key Agreement Protocol for Wireless Mobile Communications. <i>ETRI Journal</i> , 2012 , 34, 482-484	1.4	7
16	A key distribution scheme using network coding for mobile ad hoc network. <i>Security and Communication Networks</i> , 2012 , 5, 59-67	1.9	3
15	A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. <i>Security and Communication Networks</i> , 2012 , 5, 1423-1429	1.9	71
14	A new dynamic identity-based authentication protocol for multi-server environment using elliptic curve cryptography. <i>Security and Communication Networks</i> , 2012 , 5, 1260-1266	1.9	14

13	A pairing-free certificateless authenticated key agreement protocol. <i>International Journal of Communication Systems</i> , 2012 , 25, 221-230	1.7	68
12	An efficient and provably-secure certificateless signature scheme without bilinear pairings. <i>International Journal of Communication Systems</i> , 2012 , 25, 1432-1442	1.7	88
11	A more secure authentication scheme for telecare medicine information systems. <i>Journal of Medical Systems</i> , 2012 , 36, 1989-95	5.1	196
10	Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. <i>Nonlinear Dynamics</i> , 2012 , 69, 1149-1157	5	95
9	An efficient remote user authentication and key agreement protocol for mobile client-server environment from pairings. <i>Ad Hoc Networks</i> , 2012 , 10, 1009-1016	4.8	74
8	Weaknesses in a dynamic ID-based remote user authentication scheme for multi-server environment. <i>International Journal of Electronic Security and Digital Forensics</i> , 2012 , 4, 43	1	2
7	Cryptanalysis of a Smartcard-Based User Authentication Scheme for Multi-Server Environments. <i>IEICE Transactions on Communications</i> , 2012 , E95.B, 3052-3054	0.5	5
6	A new two-round certificateless authenticated key agreement protocol without bilinear pairings. <i>Mathematical and Computer Modelling</i> , 2011 , 54, 3143-3152		42
5	An ID-based proxy signature schemes without bilinear pairings. <i>Annales Des Telecommunications/Annals of Telecommunications</i> , 2011 , 66, 657-662	2	57
4	An efficient identity-based blind signature scheme without bilinear pairings. <i>Computers and Electrical Engineering</i> , 2011 , 37, 444-450	4.3	35
3	Weaknesses of a dynamic ID-based remote user authentication scheme. <i>International Journal of Electronic Security and Digital Forensics</i> , 2010 , 3, 355	1	10
2	On Diophantine equation $3a^2 + 4b^2 = 1$. <i>Annali Di Matematica Pura Ed Applicata</i> , 2010 , 189, 679-687	0.8	
1	Lattice-based undeniable signature scheme. <i>Annales Des Telecommunications/Annals of Telecommunications</i> , 1	2	2