

List of Publications by Citations

Source: <https://exaly.com/author-pdf/3179555/yi-mu-publications-by-citations.pdf>

Version: 2024-04-23

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.

233
papers

3,407
citations

28
h-index

46
g-index

248
ext. papers

4,093
ext. citations

3.2
avg, IF

5.88
L-index

#	Paper	IF	Citations
233	Certificateless Signature Revisited 2007 , 308-322		115
232	On the Security of Certificateless Signature Schemes from Asiacrypt 2003. <i>Lecture Notes in Computer Science</i> , 2005 , 13-25	0.9	113
231	Constant-Size Dynamic k-TAA. <i>Lecture Notes in Computer Science</i> , 2006 , 111-125	0.9	110
230	Server-Aided Public Key Encryption With Keyword Search. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 2833-2842	8	101
229	CP-ABE With Constant-Size Keys for Lightweight Devices. <i>IEEE Transactions on Information Forensics and Security</i> , 2014 , 9, 763-771	8	98
228	Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. <i>IEEE Transactions on Parallel and Distributed Systems</i> , 2012 , 23, 2150-2162	3.7	95
227	Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. <i>IEEE Transactions on Information Forensics and Security</i> , 2015 , 10, 665-678	8	87
226	Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding. <i>Journal of Lightwave Technology</i> , 2013 , 31, 2533-2539	4	68
225	Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. <i>Future Generation Computer Systems</i> , 2018 , 78, 720-729	7.5	64
224	Certificateless Signatures: New Schemes and Security Models. <i>Computer Journal</i> , 2012 , 55, 457-474	1.3	63
223	BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication. <i>IEEE Transactions on Information Forensics and Security</i> , 2015 , 10, 2643-2652	8	62
222	. <i>IEEE Transactions on Information Forensics and Security</i> , 2018 , 13, 2101-2113	8	55
221	Cryptanalysis of simple three-party key exchange protocol. <i>Computers and Security</i> , 2008 , 27, 16-21	4.9	54
220	Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. <i>International Journal of Information Security</i> , 2015 , 14, 307-318	2.8	53
219	Identity-based data storage in cloud computing. <i>Future Generation Computer Systems</i> , 2013 , 29, 673-681	7.5	50
218	Secure Multiparty Quantum Computation for Summation and Multiplication. <i>Scientific Reports</i> , 2016 , 6, 19655	4.9	48
217	Identity-Based Strong Designated Verifier Signature Schemes. <i>Lecture Notes in Computer Science</i> , 2004 , 313-324	0.9	45

216	Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. <i>Information Sciences</i> , 2019 , 479, 116-134	7.7	45
215	On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. <i>IEEE Transactions on Parallel and Distributed Systems</i> , 2014 , 25, 2760-2761	3.7	41
214	Identity-Based Online/Offline Encryption. <i>Lecture Notes in Computer Science</i> , 2008 , 247-261	0.9	39
213	Certificateless Threshold Ring Signature. <i>Information Sciences</i> , 2009 , 179, 3685-3696	7.7	38
212	A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. <i>Future Generation Computer Systems</i> , 2019 , 97, 284-294	7.5	37
211	. <i>IEEE Transactions on Industrial Informatics</i> , 2019 , 15, 3670-3679	11.9	37
210	Revocable Ring Signature. <i>Journal of Computer Science and Technology</i> , 2007 , 22, 785-794	1.7	37
209	A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. <i>IEEE Access</i> , 2018 , 6, 43776-43784	3.5	34
208	A New General Framework for Secure Public Key Encryption with Keyword Search. <i>Lecture Notes in Computer Science</i> , 2015 , 59-76	0.9	33
207	Comments on a Public Auditing Mechanism for Shared Cloud Data Service. <i>IEEE Transactions on Services Computing</i> , 2015 , 8, 998-999	4.8	32
206	Certificate-Based Signature: Security Model and Efficient Construction. <i>Lecture Notes in Computer Science</i> , 2007 , 110-125	0.9	32
205	Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System. <i>IEEE Access</i> , 2019 , 7, 33202-33213	3.5	28
204	Constructions of certificate-based signature secure against key replacement attacks*. <i>Journal of Computer Security</i> , 2010 , 18, 421-449	0.8	28
203	Privacy enhanced data outsourcing in the cloud. <i>Journal of Network and Computer Applications</i> , 2012 , 35, 1367-1373	7.9	27
202	Multi-User Verifiable Searchable Symmetric Encryption for Cloud Storage. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 17, 1322-1332	3.9	27
201	Strong authenticated key exchange with auxiliary inputs. <i>Designs, Codes, and Cryptography</i> , 2017 , 85, 145-173	1.2	26
200	Quantum oblivious set-member decision protocol. <i>Physical Review A</i> , 2015 , 92,	2.6	25
199	Comments on Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification□ <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 658-659	8	24

198	Distributed clinical data sharing via dynamic access-control policy transformation. <i>International Journal of Medical Informatics</i> , 2016 , 89, 25-31	5.3	24
197	Secure universal designated verifier signature without random oracles. <i>International Journal of Information Security</i> , 2008 , 7, 171-183	2.8	24
196	Practical Anonymous Divisible E-Cash from Bounded Accumulators. <i>Lecture Notes in Computer Science</i> , 2008 , 287-301	0.9	24
195	Efficient public key encryption with revocable keyword search. <i>Security and Communication Networks</i> , 2014 , 7, 466-472	1.9	23
194	An efficient quantum scheme for Private Set Intersection. <i>Quantum Information Processing</i> , 2016 , 15, 363-371	1.6	22
193	Certificateless threshold signature scheme from bilinear maps. <i>Information Sciences</i> , 2010 , 180, 4714-4728	7.7	22
192	Proxy Signature Without Random Oracles. <i>Lecture Notes in Computer Science</i> , 2006 , 473-484	0.9	22
191	Secure Channel Free ID-Based Searchable Encryption for Peer-to-Peer Group. <i>Journal of Computer Science and Technology</i> , 2016 , 31, 1012-1027	1.7	22
190	m out of n Oblivious Transfer. <i>Lecture Notes in Computer Science</i> , 2002 , 395-405	0.9	21
189	An efficient privacy-preserving aggregation and billing protocol for smart grid. <i>Security and Communication Networks</i> , 2016 , 9, 4536-4547	1.9	20
188	On security of a certificateless signcryption scheme. <i>Information Sciences</i> , 2013 , 232, 475-481	7.7	20
187	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures. <i>IEEE Transactions on Information Forensics and Security</i> , 2011 , 6, 498-512	8	20
186	How to construct identity-based signatures without the key escrow problem. <i>International Journal of Information Security</i> , 2010 , 9, 297-311	2.8	20
185	Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. <i>Lecture Notes in Computer Science</i> , 2016 , 223-239	0.9	20
184	Practical and secure telemedicine systems for user mobility. <i>Journal of Biomedical Informatics</i> , 2018 , 78, 24-32	10.2	19
183	Strongly Leakage-Resilient Authenticated Key Exchange. <i>Lecture Notes in Computer Science</i> , 2016 , 19-36	0.9	19
182	Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage. <i>Lecture Notes in Computer Science</i> , 2014 , 28-40	0.9	19
181	Provably secure server-aided verification signatures. <i>Computers and Mathematics With Applications</i> , 2011 , 61, 1705-1723	2.7	18

180	Strongly unforgeable proxy signature scheme secure in the standard model. <i>Journal of Systems and Software</i> , 2011 , 84, 1471-1479	3.3	18
179	Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain. <i>IEEE Transactions on Industrial Informatics</i> , 2020 , 16, 2677-2686	11.9	18
178	A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World. <i>Lecture Notes in Computer Science</i> , 2005 , 480-489	0.9	18
177	Continuous Leakage-Resilient Identity-Based Encryption without Random Oracles. <i>Computer Journal</i> , 2018 , 61, 586-600	1.3	17
176	Privacy-Preserving and Secure Sharing of PHR in the Cloud. <i>Journal of Medical Systems</i> , 2016 , 40, 267	5.1	17
175	Recipient Revocable Identity-Based Broadcast Encryption 2016 ,		17
174	Constant-Size Dynamic K-Times Anonymous Authentication. <i>IEEE Systems Journal</i> , 2013 , 7, 249-261	4.3	17
173	Universal Designated Verifier Signature Without Delegatability. <i>Lecture Notes in Computer Science</i> , 2006 , 479-498	0.9	17
172	Efficient identity-based online/offline encryption and signcryption with short ciphertext. <i>International Journal of Information Security</i> , 2017 , 16, 299-311	2.8	16
171	Private Keyword-Search for Database Systems Against Insider Attacks. <i>Journal of Computer Science and Technology</i> , 2017 , 32, 599-617	1.7	16
170	Cloud-based Outsourcing for Enabling Privacy-Preserving Large-scale Non-Negative Matrix Factorization. <i>IEEE Transactions on Services Computing</i> , 2019 , 1-1	4.8	16
169	Subset Membership Encryption and Its Applications to Oblivious Transfer. <i>IEEE Transactions on Information Forensics and Security</i> , 2014 , 9, 1098-1107	8	16
168	Identity-based provable data possession revisited: Security analysis and generic construction. <i>Computer Standards and Interfaces</i> , 2017 , 54, 10-19	3.5	16
167	Trust-oriented QoS-aware composite service selection based on genetic algorithms. <i>Concurrency Computation Practice and Experience</i> , 2014 , 26, 500-515	1.4	16
166	CCA2 secure public-key encryption scheme tolerating continual leakage attacks. <i>Security and Communication Networks</i> , 2016 , 9, 4505-4519	1.9	15
165	On the Security of an Efficient and Robust Certificateless Signature Scheme for IIoT Environments. <i>IEEE Access</i> , 2019 , 7, 91074-91079	3.5	15
164	Fully Secure Lightweight Certificateless Signature Scheme for IIoT. <i>IEEE Access</i> , 2019 , 7, 144433-144443	3.5	15
163	Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs. <i>IEEE Transactions on Information Forensics and Security</i> , 2014 , 9, 5-13	8	15

162	A robust trust model for service-oriented systems. <i>Journal of Computer and System Sciences</i> , 2013 , 79, 596-608	1	15
161	Short (Identity-Based) Strong Designated Verifier Signature Schemes. <i>Lecture Notes in Computer Science</i> , 2006 , 214-225	0.9	15
160	Provably Secure Identity Based Provable Data Possession. <i>Lecture Notes in Computer Science</i> , 2015 , 310-325	3.5	14
159	Identity-Based On-Line/Off-Line Signcryption 2008 ,		14
158	Anonymous Identity-Based Broadcast Encryption with Adaptive Security. <i>Lecture Notes in Computer Science</i> , 2013 , 258-271	0.9	14
157	Identity-Based Universal Designated Verifier Signatures. <i>Lecture Notes in Computer Science</i> , 2005 , 825-834	3.9	14
156	A New Signature Scheme Without Random Oracles from Bilinear Pairings. <i>Lecture Notes in Computer Science</i> , 2006 , 67-80	0.9	14
155	Proof of retrievability with public verifiability resilient against related-key attacks. <i>IET Information Security</i> , 2015 , 9, 43-49	1.4	13
154	Improving Privacy-Preserving and Security for Decentralized Key-Policy Attributed-Based Encryption. <i>IEEE Access</i> , 2018 , 6, 12736-12745	3.5	13
153	Online/Offline Ciphertext Retrieval on Resource Constrained Devices. <i>Computer Journal</i> , 2016 , 59, 955-969	6.9	13
152	Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city. <i>Personal and Ubiquitous Computing</i> , 2017 , 21, 855-868	2.1	13
151	Leakage Resilient Authenticated Key Exchange Secure in the Auxiliary Input Model. <i>Lecture Notes in Computer Science</i> , 2013 , 204-217	0.9	13
150	Privacy-Preserved Access Control for Cloud Computing 2011 ,		13
149	Practical RFID ownership transfer scheme. <i>Journal of Computer Security</i> , 2011 , 19, 319-341	0.8	13
148	Three-Round Secret Handshakes Based on ElGamal and DSA. <i>Lecture Notes in Computer Science</i> , 2006 , 332-342	0.9	13
147	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. <i>IEEE Systems Journal</i> , 2017 , 11, 1018-1026	4.3	12
146	Cryptanalysis and improvement of an efficient certificateless signature scheme. <i>Journal of Communications and Networks</i> , 2008 , 10, 10-17	4.1	12
145	Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world		12

144	Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. <i>IEEE Systems Journal</i> , 2020 , 14, 387-397	4.3	12
143	A Generic Scheme of plaintext-checkable database encryption. <i>Information Sciences</i> , 2018 , 429, 88-101	7.7	12
142	Provably Secure Homomorphic Signcryption. <i>Lecture Notes in Computer Science</i> , 2017 , 349-360	0.9	11
141	Privacy-Preserving Certificateless Cloud Auditing with Multiple Users. <i>Wireless Personal Communications</i> , 2019 , 106, 1161-1182	1.9	11
140	Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. <i>International Journal of Information Security</i> , 2018 , 17, 463-475	2.8	11
139	A Secure IPv6 Address Configuration Protocol for Vehicular Networks. <i>Wireless Personal Communications</i> , 2014 , 79, 721-744	1.9	11
138	EVA: Efficient Versatile Auditing Scheme for IoT-Based Datamarket in Jointcloud. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 882-892	10.7	11
137	Comment on Secure quantum private information retrieval using phase-encoded queries <i>Physical Review A</i> , 2016 , 94,	2.6	11
136	One-Round Privacy-Preserving Meeting Location Determination for Smartphone Applications. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 1712-1721	8	11
135	Multiauthority Access Control With Anonymous Authentication for Personal Health Record. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 156-167	10.7	11
134	Scalable and redactable blockchain with update and anonymity. <i>Information Sciences</i> , 2021 , 546, 25-41	7.7	11
133	AAC-OT: Accountable Oblivious Transfer With Access Control. <i>IEEE Transactions on Information Forensics and Security</i> , 2015 , 10, 2502-2514	8	10
132	Privacy-Preserving Multi-Authority Attribute-Based Data Sharing Framework for Smart Grid. <i>IEEE Access</i> , 2020 , 8, 23294-23307	3.5	10
131	Witness-based searchable encryption. <i>Information Sciences</i> , 2018 , 453, 364-378	7.7	10
130	Securing wireless mesh networks with ticket-based authentication 2008 ,		10
129	Robust non-interactive oblivious transfer. <i>IEEE Communications Letters</i> , 2003 , 7, 153-155	3.8	10
128	Policy-Driven Blockchain and Its Applications for Transport Systems. <i>IEEE Transactions on Services Computing</i> , 2019 , 1-1	4.8	9
127	Membership Encryption and Its Applications. <i>Lecture Notes in Computer Science</i> , 2013 , 219-234	0.9	9

126	Dynamic Trust Model for Federated Identity Management 2010 ,		9
125	A Generic Construction of Identity-Based Online/Offline Signcryption 2008 ,		9
124	Improved Identity-Based Online/Offline Encryption. <i>Lecture Notes in Computer Science</i> , 2015 , 160-173	0.9	9
123	Privacy-Preserving Cloud Auditing with Multiple Uploaders. <i>Lecture Notes in Computer Science</i> , 2016 , 224-237	0.9	9
122	Multicopy provable data possession scheme supporting data dynamics for cloud-based Electronic Medical Record system. <i>Information Sciences</i> , 2021 , 545, 254-276	7.7	9
121	A Fair Electronic Cash Scheme. <i>Lecture Notes in Computer Science</i> , 2001 , 20-32	0.9	9
120	A New Public Remote Integrity Checking Scheme with User Privacy. <i>Lecture Notes in Computer Science</i> , 2015 , 377-394	0.9	8
119	Security of Grouping-Proof Authentication Protocol for Distributed RFID Systems. <i>IEEE Wireless Communications Letters</i> , 2018 , 7, 254-257	5.9	8
118	Designated Verifier Proxy Re-signature for Deniable and Anonymous Wireless Communications. <i>Wireless Personal Communications</i> , 2017 , 97, 3017-3030	1.9	8
117	Two Quantum Protocols for Oblivious Set-member Decision Problem. <i>Scientific Reports</i> , 2015 , 5, 15914	4.9	8
116	An Expressive Test-Decrypt-Verify Attribute-Based Encryption Scheme With Hidden Policy for Smart Medical Cloud. <i>IEEE Systems Journal</i> , 2021 , 15, 365-376	4.3	8
115	Privacy-enhanced attribute-based private information retrieval. <i>Information Sciences</i> , 2018 , 454-455, 275-291	7.7	7
114	A resilient identity-based authenticated key exchange protocol. <i>Security and Communication Networks</i> , 2015 , 8, 2279-2290	1.9	7
113	Provably Secure Single Sign-on Scheme in Distributed Systems and Networks 2012 ,		7
112	Optimal Online/Offline Signature: How to Sign a Message without Online Computation. <i>Lecture Notes in Computer Science</i> , 2008 , 98-111	0.9	7
111	Ad Hoc Group Signatures. <i>Lecture Notes in Computer Science</i> , 2006 , 120-135	0.9	7
110	Efficient Micropayment of Cryptocurrency from Blockchains. <i>Computer Journal</i> , 2019 , 62, 507-517	1.3	7
109	The generic construction of continuous leakage-resilient identity-based cryptosystems. <i>Theoretical Computer Science</i> , 2019 , 772, 1-45	1.1	7

108	Introduction to Security Reduction 2018 ,		7
107	Secure-channel free keyword search with authorization in manager-centric databases. <i>Computers and Security</i> , 2017 , 69, 50-64	4.9	6
106	Identity-based quotable ring signature. <i>Information Sciences</i> , 2015 , 321, 71-89	7.7	6
105	Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage. <i>IEEE Access</i> , 2020 , 8, 104344-104356	3.5	6
104	New Approach for Privacy-Aware Location-Based Service Communications. <i>Wireless Personal Communications</i> , 2018 , 101, 1057-1073	1.9	6
103	Provably Secure (Broadcast) Homomorphic Signcryption. <i>International Journal of Foundations of Computer Science</i> , 2019 , 30, 511-529	0.6	6
102	Identity based identification from algebraic coding theory. <i>Theoretical Computer Science</i> , 2014 , 520, 51-61	1	6
101	Fuzzy Extractors for Biometric Identification 2017 ,		6
100	Efficient E-coupon systems with strong user privacy. <i>Telecommunication Systems</i> , 2017 , 64, 695-708	2.3	6
99	Towards a cryptographic treatment of publish/subscribe systems ¹ . <i>Journal of Computer Security</i> , 2014 , 22, 33-67	0.8	6
98	Privacy-Preserving Authorized RFID Authentication Protocols. <i>Lecture Notes in Computer Science</i> , 2014 , 108-122	0.9	6
97	Case-Based Trust Evaluation from Provenance Information 2011 ,		6
96	Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. <i>Theoretical Computer Science</i> , 2019 , 767, 51-72	1.1	6
95	Strongly leakage resilient authenticated key exchange, revisited. <i>Designs, Codes, and Cryptography</i> , 2019 , 87, 2885-2911	1.2	5
94	Privacy-Preserving Yoking Proof with Key Exchange in the Three-Party Setting. <i>Wireless Personal Communications</i> , 2017 , 94, 1017-1034	1.9	5
93	A secure mobility support scheme for 6LoWPAN wireless sensor networks. <i>Security and Communication Networks</i> , 2014 , 7, 641-652	1.9	5
92	Efficient oblivious transfers with access control. <i>Computers and Mathematics With Applications</i> , 2012 , 63, 827-837	2.7	5
91	Compact Anonymous Hierarchical Identity-Based Encryption with Constant Size Private Keys. <i>Computer Journal</i> , 2016 , 59, 452-461	1.3	5

90	Secure Outsourced Attribute-based Sharing Framework for Lightweight Devices in Smart Health Systems. <i>IEEE Transactions on Services Computing</i> , 2021 , 1-1	4.8	5
89	Improving Privacy-Preserving CP-ABE with Hidden Access Policy. <i>Lecture Notes in Computer Science</i> , 2018 , 596-605	0.9	5
88	Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. <i>Quantum Information Processing</i> , 2017 , 16, 1	1.6	4
87	Continuous leakage-resilient identity-based encryption with leakage amplification. <i>Designs, Codes, and Cryptography</i> , 2019 , 87, 2061-2090	1.2	4
86	Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost. <i>Theoretical Computer Science</i> , 2018 , 714, 15-26	1.1	4
85	Comments on [Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks] <i>IEEE Transactions on Wireless Communications</i> , 2016 , 15, 3097-3099	9.6	4
84	Privacy-Preserving Mutual Authentication in RFID with Designated Readers. <i>Wireless Personal Communications</i> , 2017 , 96, 4819-4845	1.9	4
83	Policy-controlled signatures and their applications. <i>Computer Standards and Interfaces</i> , 2017 , 50, 26-41	3.5	4
82	Vulnerabilities of an ECC-based RFID authentication scheme. <i>Security and Communication Networks</i> , 2015 , 8, 3262-3270	1.9	4
81	Optimistic Fair Exchange with Strong Resolution-Ambiguity. <i>IEEE Journal on Selected Areas in Communications</i> , 2011 , 29, 1491-1502	14.2	4
80	PBTrust: A Priority-Based Trust Model for Service Selection in General Service-Oriented Environments 2010 ,		4
79	An Efficient Certificateless Encryption Scheme in the Standard Model 2009 ,		4
78	Hierarchical Identity-Based Online/Offline Encryption 2008 ,		4
77	GTrust: An Innovated Trust Model for Group Services Selection in Web-Based Service-Oriented Environments. <i>Lecture Notes in Computer Science</i> , 2011 , 306-313	0.9	4
76	Anonymous and Updatable Identity-Based Hash Proof System. <i>IEEE Systems Journal</i> , 2019 , 13, 2818-2829	4.3	4
75	Privacy-enhanced remote data integrity checking with updatable timestamp. <i>Information Sciences</i> , 2020 , 527, 210-226	7.7	4
74	Secure and Efficient Data Aggregation for IoT Monitoring Systems. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 8056-8063	10.7	4
73	. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2021 , 18, 563-575	3.9	4

72	Trust-based group services selection in web-based service-oriented environments. <i>World Wide Web</i> , 2016 , 19, 807-832	2.9	3
71	Privacy-preserving data search and sharing protocol for social networks through wireless applications. <i>Concurrency Computation Practice and Experience</i> , 2017 , 29, e3870	1.4	3
70	ACE with Compact Ciphertext Size and Decentralized Sanitizers. <i>International Journal of Foundations of Computer Science</i> , 2019 , 30, 531-549	0.6	3
69	Key management for Smart Grid based on asymmetric key-wrapping. <i>International Journal of Computer Mathematics</i> , 2015 , 92, 498-512	1.2	3
68	A code-based signature scheme from the Lyubashevsky framework. <i>Theoretical Computer Science</i> , 2020 , 835, 15-30	1.1	3
67	Authenticated Data Redaction with Accountability and Transparency. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020 , 1-1	3.9	3
66	Anonymous Proxy Signature with Restricted Traceability 2014 ,		3
65	Efficient RFID Authentication Scheme for Supply Chain Applications 2010 ,		3
64	Web Service Selection Based on Similarity Evaluation 2011 ,		3
63	Multi-identity management for identity-based cryptography. <i>Journal of Discrete Mathematical Sciences and Cryptography</i> , 2008 , 11, 639-672	1.7	3
62	Certificateless Designated Verifier Signature Schemes 2006 ,		3
61	Universal Designated Verifier Signatures with Threshold-Signers. <i>Lecture Notes in Computer Science</i> , 2009 , 89-109	0.9	3
60	A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. <i>Information Sciences</i> , 2020 , 516, 331-345	7.7	3
59	Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. <i>Theoretical Computer Science</i> , 2020 , 809, 277-295	1.1	3
58	Threshold privacy-preserving cloud auditing with multiple uploaders. <i>International Journal of Information Security</i> , 2019 , 18, 321-331	2.8	3
57	An Enhanced Certificateless Aggregate Signature Without Pairings for E-Healthcare System. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 5000-5008	10.7	3
56	Strong Identity-Based Proxy Signature Schemes, Revisited. <i>Wireless Communications and Mobile Computing</i> , 2018 , 2018, 1-11	1.9	3
55	Efficient dynamic threshold identity-based encryption with constant-size ciphertext. <i>Theoretical Computer Science</i> , 2016 , 609, 49-59	1.1	2

54	Loss-Tolerant Bundle Fragment Authentication for Space-Based DTNs. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2015 , 12, 615-625	3.9	2
53	Multi-authority security framework for scalable EHR systems. <i>International Journal of Medical Engineering and Informatics</i> , 2016 , 8, 390	0.5	2
52	Efficient and secure image authentication with robustness and versatility. <i>Science China Information Sciences</i> , 2020 , 63, 1	3.4	2
51	A New Revocable and Re-Delegable Proxy Signature and Its Application. <i>Journal of Computer Science and Technology</i> , 2018 , 33, 380-399	1.7	2
50	Policy controlled system with anonymity. <i>Theoretical Computer Science</i> , 2018 , 745, 87-113	1.1	2
49	Security pitfalls of an efficient threshold proxy signature scheme for mobile agents. <i>Information Processing Letters</i> , 2014 , 114, 5-8	0.8	2
48	Public-Key Encryption Resilient against Linear Related-Key Attacks Revisited 2014 ,		2
47	Short Signatures with a Tighter Security Reduction Without Random Oracles. <i>Computer Journal</i> , 2011 , 54, 513-524	1.3	2
46	Secure Mobile Agents with Designated Hosts 2009 ,		2
45	Server-Aided Public Key Generation Protocols on Low-power Devices for Ad-hoc Networks 2006 ,		2
44	Privacy-enhanced Internet storage		2
43	Blockchain-based random auditor committee for integrity verification. <i>Future Generation Computer Systems</i> , 2022 , 131, 183-193	7.5	2
42	Proxy Signature with Revocation. <i>Lecture Notes in Computer Science</i> , 2016 , 21-36	0.9	2
41	Relations between robustness and RKA security under public-key encryption. <i>Theoretical Computer Science</i> , 2016 , 628, 78-91	1.1	2
40	Privacy-Preserving Reverse Nearest Neighbor Query over Encrypted Spatial Data. <i>IEEE Transactions on Services Computing</i> , 2021 , 1-1	4.8	2
39	Distributed Ciphertext-Policy Attribute-Based Encryption With Enhanced Collusion Resilience and Privacy Preservation. <i>IEEE Systems Journal</i> , 2021 , 1-12	4.3	2
38	A Novel Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Anonymous Key Generation. <i>Lecture Notes in Computer Science</i> , 2018 , 435-446	0.9	2
37	Privacy-Preserving Flexible Access Control for Encrypted Data in Internet of Things. <i>IEEE Internet of Things Journal</i> , 2021 , 8, 14731-14745	10.7	2

36	A Generic Table Recomputation-Based Higher-Order Masking. <i>IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems</i> , 2017 , 36, 1779-1789	2.5	1
35	Top-Level Secure Certificateless Signature Against Malicious-But-Passive KGC. <i>IEEE Access</i> , 2019 , 7, 112879-112878	3.5	1
34	Secure and Privacy-Preserving Attribute-Based Sharing Framework in Vehicles Ad Hoc Networks. <i>IEEE Access</i> , 2020 , 8, 116781-116795	3.5	1
33	An improved Durandal signature scheme. <i>Science China Information Sciences</i> , 2020 , 63, 1	3.4	1
32	Fully Secure Hierarchical Inner Product Encryption for Privacy Preserving Keyword Searching in Cloud 2015 ,		1
31	New constructions of OSBE schemes and their applications in oblivious access control. <i>International Journal of Information Security</i> , 2012 , 11, 389-401	2.8	1
30	Identity-Based Mediated RSA Revisited 2013 ,		1
29	Secure mobile agents with controlled resources. <i>Concurrency Computation Practice and Experience</i> , 2011 , 23, 1348-1366	1.4	1
28	Secure Decentralized Attribute-Based Sharing of Personal Health Records with Blockchain. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	1
27	HUCDO. <i>ACM Transactions on Cyber-Physical Systems</i> , 2020 , 4, 1-23	2.3	1
26	Novel updatable identity-based hash proof system and its applications. <i>Theoretical Computer Science</i> , 2020 , 804, 1-28	1.1	1
25	Secure Data Sharing With Lightweight Computation in E-Health. <i>IEEE Access</i> , 2020 , 8, 209630-209643	3.5	1
24	Novel generic construction of leakage-resilient PKE scheme with CCA security. <i>Designs, Codes, and Cryptography</i> , 2021 , 89, 1575	1.2	1
23	Privacy-Aware Image Authentication from Cryptographic Primitives. <i>Computer Journal</i> , 2021 , 64, 1178-1192	1.5	1
22	Secure and Privacy-Preserved Data Collection for IoT Wireless Sensors. <i>IEEE Internet of Things Journal</i> , 2021 , 1-1	10.7	1
21	Efficient Traceable Oblivious Transfer and Its Applications. <i>Lecture Notes in Computer Science</i> , 2018 , 610-621	6.9	1
20	Bidirectional and Malleable Proof-of-Ownership for Large File in Cloud Storage. <i>IEEE Transactions on Cloud Computing</i> , 2021 , 1-1	3.3	1
19	An IPv6-based mobility framework for urban vehicular networks. <i>International Journal of Network Management</i> , 2015 , 25, 141-158	1.8	0

18	Controllable software licensing system for sub-licensing. <i>Journal of Information Security and Applications</i> , 2022 , 64, 103061	3.5	○
17	Black-Box Accountable Authority Identity-Based Revocation System. <i>Computer Journal</i> , 2020 , 63, 525-535	3.3	○
16	Unlinkable and Revocable Secret Handshake. <i>Computer Journal</i> , 2021 , 64, 1303-1314	1.3	○
15	Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT. <i>IEEE Transactions on Cloud Computing</i> , 2021 , 1-1	3.3	○
14	Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud. <i>Journal of Systems Architecture</i> , 2022 , 102569	5.5	○
13	Generalized closest substring encryption. <i>Designs, Codes, and Cryptography</i> , 2016 , 80, 103-124	1.2	
12	A new generic construction of anonymous designated confirmer signature for privacy-preserving fair exchange. <i>International Journal of Computer Mathematics</i> , 2017 , 94, 946-961	1.2	
11	Privacy-Preserving Data Packet Filtering Protocol with Source IP Authentication. <i>Wireless Personal Communications</i> , 2017 , 95, 3509-3537	1.9	
10	Publicly verifiable secure communication with user and data privacy. <i>Personal and Ubiquitous Computing</i> , 2019 , 1	2.1	
9	Further ideal multipartite access structures from integer polymatroids. <i>Science China Information Sciences</i> , 2015 , 58, 1-13	3.4	
8	Privacy preserving protocol for service aggregation in cloud computing. <i>Software - Practice and Experience</i> , 2012 , 42, 467-483	2.5	
7	Efficient and secure stored-value cards with leakage resilience. <i>Computers and Electrical Engineering</i> , 2012 , 38, 370-380	4.3	
6	Further Analysis of a Practical Hierarchical Identity-Based Encryption Scheme. <i>IEICE Transactions on Information and Systems</i> , 2012 , E95.D, 1690-1693	0.6	
5	Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacrpt004. <i>Journal of Computer Science and Technology</i> , 2007 , 22, 71-74	1.7	
4	Short Group Signatures Without Random Oracles. <i>Journal of Computer Science and Technology</i> , 2007 , 22, 805-821	1.7	
3	Secure and Efficient General Circuits Attribute-Based Access Control in Cloud Computing. <i>IEEE Systems Journal</i> , 2022 , 1-11	4.3	
2	BA2P : Bidirectional and Anonymous Auction Protocol with Dispute-Freeness. <i>Security and Communication Networks</i> , 2021 , 2021, 1-12	1.9	
1	On the Security of Symmetric Encryption Against Mass Surveillance. <i>IEEE Access</i> , 2020 , 8, 175625-175636	3.5	

