Yi Mu

List of Publications by Year in descending order

246 papers	5,062 citations	117453 34 h-index	149479 56 g-index
248 all docs	248 docs citations	248 times ranked	2719 citing authors

#	Article	IF	Citations
1	On the Security of Certificateless Signature Schemes from Asiacrypt 2003. Lecture Notes in Computer Science, 2005, , 13-25.	1.0	174
2	Certificateless Signature Revisited. , 2007, , 308-322.		169
3	Constant-Size Dynamic k-TAA. Lecture Notes in Computer Science, 2006, , 111-125.	1.0	148
4	Server-Aided Public Key Encryption With Keyword Search. IEEE Transactions on Information Forensics and Security, 2016, 11, 2833-2842.	4.5	140
5	CP-ABE With Constant-Size Keys for Lightweight Devices. IEEE Transactions on Information Forensics and Security, 2014, 9, 763-771.	4.5	133
6	Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems, 2012, 23, 2150-2162.	4.0	126
7	Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. IEEE Transactions on Information Forensics and Security, 2015, 10, 665-678.	4.5	117
8	Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems, 2018, 78, 720-729.	4.9	94
9	BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication. IEEE Transactions on Information Forensics and Security, 2015, 10, 2643-2652.	4.5	91
10	Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding. Journal of Lightwave Technology, 2013, 31, 2533-2539.	2.7	88
11	Identity-based data storage in cloud computing. Future Generation Computer Systems, 2013, 29, 673-681.	4.9	83
12	Identity-Based Strong Designated Verifier Signature Schemes. Lecture Notes in Computer Science, 2004, , 313-324.	1.0	82
13	Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud. IEEE Transactions on Information Forensics and Security, 2018, 13, 2101-2113.	4.5	81
14	Cryptanalysis of simple three-party key exchange protocol. Computers and Security, 2008, 27, 16-21.	4.0	75
15	Certificateless Signatures: New Schemes and Security Models. Computer Journal, 2012, 55, 457-474.	1.5	72
16	Secure Multiparty Quantum Computation for Summation and Multiplication. Scientific Reports, 2016, 6, 19655.	1.6	71
17	Building Redactable Consortium Blockchain for Industrial Internet-of-Things. IEEE Transactions on Industrial Informatics, 2019, 15, 3670-3679.	7.2	67
18	Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. International Journal of Information Security, 2015, 14, 307-318.	2.3	64

#	Article	IF	Citations
19	Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. Information Sciences, 2019, 479, 116-134.	4.0	64
20	On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 2760-2761.	4.0	59
21	A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. Future Generation Computer Systems, 2019, 97, 284-294.	4.9	56
22	Certificate-Based Signature: Security Model and Efficient Construction. Lecture Notes in Computer Science, 2007, , 110-125.	1.0	54
23	Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System. IEEE Access, 2019, 7, 33202-33213.	2.6	52
24	Multi-User Verifiable Searchable Symmetric Encryption for Cloud Storage. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 1322-1332.	3.7	50
25	Revocable Ring Signature. Journal of Computer Science and Technology, 2007, 22, 785-794.	0.9	48
26	Identity-Based Online/Offline Encryption. Lecture Notes in Computer Science, 2008, , 247-261.	1.0	48
27	Certificateless Threshold Ring Signature. Information Sciences, 2009, 179, 3685-3696.	4.0	48
28	Proxy Signature Without Random Oracles. Lecture Notes in Computer Science, 2006, , 473-484.	1.0	44
29	A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. IEEE Access, 2018, 6, 43776-43784.	2.6	42
30	Scalable and redactable blockchain with update and anonymity. Information Sciences, 2021, 546, 25-41.	4.0	40
31	A New General Framework for Secure Public Key Encryption with Keyword Search. Lecture Notes in Computer Science, 2015, , 59-76.	1.0	40
32	Comments on a Public Auditing Mechanism for Shared Cloud Data Service. IEEE Transactions on Services Computing, 2015, 8, 998-999.	3.2	37
33	Distributed clinical data sharing via dynamic access-control policy transformation. International Journal of Medical Informatics, 2016, 89, 25-31.	1.6	37
34	Multicopy provable data possession scheme supporting data dynamics for cloud-based Electronic Medical Record system. Information Sciences, 2021, 545, 254-276.	4.0	36
35	Privacy enhanced data outsourcing in the cloud. Journal of Network and Computer Applications, 2012, 35, 1367-1373.	5.8	35
36	On security of a certificateless signcryption scheme. Information Sciences, 2013, 232, 475-481.	4.0	34

#	Article	IF	Citations
37	Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. IEEE Systems Journal, 2020, 14, 387-397.	2.9	34
38	Practical Anonymous Divisible E-Cash from Bounded Accumulators. Lecture Notes in Computer Science, 2008, , 287-301.	1.0	34
39	An efficient quantum scheme for Private Set Intersection. Quantum Information Processing, 2016, 15, 363-371.	1.0	33
40	Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain. IEEE Transactions on Industrial Informatics, 2020, 16, 2677-2686.	7.2	33
41	Identity-Based Ring Signcryption Schemes: Cryptographic Primitives for Preserving Privacy and Authenticity in the Ubiquitous World. , 0, , .		32
42	Constructions of certificate-based signature secure against key replacement attacks*. Journal of Computer Security, 2010, 18, 421-449.	0.5	32
43	An efficient privacyâ€preserving aggregation and billing protocol for smart grid. Security and Communication Networks, 2016, 9, 4536-4547.	1.0	32
44	Practical and secure telemedicine systems for user mobility. Journal of Biomedical Informatics, 2018, 78, 24-32.	2.5	32
45	A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World. Lecture Notes in Computer Science, 2005, , 480-489.	1.0	32
46	Quantum oblivious set-member decision protocol. Physical Review A, 2015, 92, .	1.0	31
47	How to construct identity-based signatures without the key escrow problem. International Journal of Information Security, 2010, 9, 297-311.	2.3	30
48	Efficient public key encryption with revocable keyword search. Security and Communication Networks, 2014, 7, 466-472.	1.0	29
49	Strong authenticated key exchange with auxiliary inputs. Designs, Codes, and Cryptography, 2017, 85, 145-173.	1.0	29
50	Fully Secure Lightweight Certificateless Signature Scheme for IIoT. IEEE Access, 2019, 7, 144433-144443.	2.6	29
51	Certificateless threshold signature scheme from bilinear maps. Information Sciences, 2010, 180, 4714-4728.	4.0	28
52	Secure Channel Free ID-Based Searchable Encryption for Peer-to-Peer Group. Journal of Computer Science and Technology, 2016, 31, 1012-1027.	0.9	28
53	Privacy-Preserving and Secure Sharing of PHR in the Cloud. Journal of Medical Systems, 2016, 40, 267.	2.2	27
54	Multiauthority Access Control With Anonymous Authentication for Personal Health Record. IEEE Internet of Things Journal, 2021, 8, 156-167.	5.5	27

#	Article	IF	Citations
55	m out of n Oblivious Transfer. Lecture Notes in Computer Science, 2002, , 395-405.	1.0	27
56	Secure universal designated verifier signature without random oracles. International Journal of Information Security, 2008, 7, 171-183.	2.3	26
57	Constant-Size Dynamic k-Times Anonymous Authentication. IEEE Systems Journal, 2013, 7, 249-261.	2.9	26
58	Continuous Leakage-Resilient Identity-Based Encryption without Random Oracles. Computer Journal, 2018, 61, 586-600.	1.5	26
59	Comments on â€œPublic Integrity Auditing for Dynamic Data Sharing With Multiuser Modificationâ€• IEEE Transactions on Information Forensics and Security, 2016, 11, 658-659.	4.5	25
60	Cloud-Based Outsourcing for Enabling Privacy-Preserving Large-Scale Non-Negative Matrix Factorization. IEEE Transactions on Services Computing, 2022, 15, 266-278.	3.2	25
61	Short (Identity-Based) Strong Designated Verifier Signature Schemes. Lecture Notes in Computer Science, 2006, , 214-225.	1.0	25
62	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures. IEEE Transactions on Information Forensics and Security, 2011, 6, 498-512.	4.5	24
63	Provably secure server-aided verification signatures. Computers and Mathematics With Applications, 2011, 61, 1705-1723.	1.4	24
64	Trustâ€oriented QoSâ€aware composite service selection based on genetic algorithms. Concurrency Computation Practice and Experience, 2014, 26, 500-515.	1.4	24
65	Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. Lecture Notes in Computer Science, 2016, , 223-239.	1.0	24
66	Recipient Revocable Identity-Based Broadcast Encryption. , 2016, , .		24
67	Privacy-Preserving Multi-Authority Attribute-Based Data Sharing Framework for Smart Grid. IEEE Access, 2020, 8, 23294-23307.	2.6	24
68	Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage. Lecture Notes in Computer Science, 2014, , 28-40.	1.0	23
69	A New Signature Scheme Without Random Oracles from Bilinear Pairings. Lecture Notes in Computer Science, 2006, , 67-80.	1.0	23
70	Strongly unforgeable proxy signature scheme secure in the standard model. Journal of Systems and Software, 2011, 84, 1471-1479.	3.3	22
71	Efficient identity-based online/offline encryption and signcryption with short ciphertext. International Journal of Information Security, 2017, 16, 299-311.	2.3	21
72	Private Keyword-Search for Database Systems Against Insider Attacks. Journal of Computer Science and Technology, 2017, 32, 599-617.	0.9	21

#	Article	IF	Citations
73	Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city. Personal and Ubiquitous Computing, 2017, 21, 855-868.	1.9	21
74	On the Security of an Efficient and Robust Certificateless Signature Scheme for IIoT Environments. IEEE Access, 2019, 7, 91074-91079.	2.6	21
75	Privacy-Preserved Access Control for Cloud Computing. , 2011, , .		20
76	A robust trust model for service-oriented systems. Journal of Computer and System Sciences, 2013, 79, 596-608.	0.9	20
77	Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs. IEEE Transactions on Information Forensics and Security, 2014, 9, 5-13.	4.5	20
78	Strongly Leakage-Resilient Authenticated Key Exchange. Lecture Notes in Computer Science, 2016, , 19-36.	1.0	20
79	Fuzzy Extractors for Biometric Identification. , 2017, , .		20
80	Subset Membership Encryption and Its Applications to Oblivious Transfer. IEEE Transactions on Information Forensics and Security, 2014, 9, 1098-1107.	4.5	19
81	Online/Offline Ciphertext Retrieval on Resource Constrained Devices. Computer Journal, 2016, 59, 955-969.	1.5	19
82	Privacy-Preserving Certificateless Cloud Auditing with Multiple Users. Wireless Personal Communications, 2019, 106, 1161-1182.	1.8	19
83	EVA: Efficient Versatile Auditing Scheme for IoT-Based Datamarket in Jointcloud. IEEE Internet of Things Journal, 2020, 7, 882-892.	5.5	19
84	An Expressive â€œTest-Decrypt-Verifyâ€•Attribute-Based Encryption Scheme With Hidden Policy for Smart Medical Cloud. IEEE Systems Journal, 2021, 15, 365-376.	2.9	19
85	Identity-Based Universal Designated Verifier Signatures. Lecture Notes in Computer Science, 2005, , 825-834.	1.0	19
86	Practical RFID ownership transfer scheme. Journal of Computer Security, 2011, 19, 319-341.	0.5	18
87	CCA2 secure publicâ€key encryption scheme tolerating continual leakage attacks. Security and Communication Networks, 2016, 9, 4505-4519.	1.0	18
88	Identity-based provable data possession revisited: Security analysis and generic construction. Computer Standards and Interfaces, 2017, 54, 10-19.	3.8	18
89	Improving Privacy-Preserving and Security for Decentralized Key-Policy Attributed-Based Encryption. IEEE Access, 2018, 6, 12736-12745.	2.6	18
90	Secure and Efficient Data Aggregation for IoT Monitoring Systems. IEEE Internet of Things Journal, 2021, 8, 8056-8063.	5.5	18

#	Article	IF	Citations
91	Blockchain-based random auditor committee for integrity verification. Future Generation Computer Systems, 2022, 131, 183-193.	4.9	18
92	Certificateless Designated Verifier Signature Schemes. , 2006, , .		17
93	Proof of retrievability with public verifiability resilient against relatedâ€key attacks. IET Information Security, 2015, 9, 43-49.	1.1	17
94	Universal Designated Verifier Signature Without Delegatability. Lecture Notes in Computer Science, 2006, , 479-498.	1.0	17
95	Identity-Based On-Line/Off-Line Signcryption. , 2008, , .		16
96	Provably Secure Identity Based Provable Data Possession. Lecture Notes in Computer Science, 2015, , 310-325.	1.0	16
97	One-Round Privacy-Preserving Meeting Location Determination for Smartphone Applications. IEEE Transactions on Information Forensics and Security, 2016, 11, 1712-1721.	4.5	16
98	Efficient Micropayment of Cryptocurrency from Blockchains. Computer Journal, 2019, 62, 507-517.	1.5	16
99	An Enhanced Certificateless Aggregate Signature Without Pairings for E-Healthcare System. IEEE Internet of Things Journal, 2021, 8, 5000-5008.	5.5	16
100	Anonymous Identity-Based Broadcast Encryption with Adaptive Security. Lecture Notes in Computer Science, 2013, , 258-271.	1.0	16
101	A Secure IPv6 Address Configuration Protocol for Vehicular Networks. Wireless Personal Communications, 2014, 79, 721-744.	1.8	15
102	A Generic Scheme of plaintext-checkable database encryption. Information Sciences, 2018, 429, 88-101.	4.0	15
103	Introduction to Security Reduction. , 2018, , .		15
104	Secure Outsourced Attribute-Based Sharing Framework for Lightweight Devices in Smart Health Systems. IEEE Transactions on Services Computing, 2022, 15, 3019-3030.	3.2	15
105	Leakage Resilient Authenticated Key Exchange Secure in the Auxiliary Input Model. Lecture Notes in Computer Science, 2013, , 204-217.	1.0	14
106	Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. International Journal of Information Security, 2018, 17, 463-475.	2.3	14
107	Policy-Driven Blockchain and Its Applications for Transport Systems. IEEE Transactions on Services Computing, 2019, , 1-1.	3.2	14
108	Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. Theoretical Computer Science, 2019, 767, 51-72.	0.5	14

#	Article	IF	Citations
109	Secure Decentralized Attribute-Based Sharing of Personal Health Records With Blockchain. IEEE Internet of Things Journal, 2022, 9, 12482-12496.	5.5	14
110	Cryptanalysis and improvement of an efficient certificateless signature scheme. Journal of Communications and Networks, 2008, 10, 10-17.	1.8	13
111	Securing wireless mesh networks with ticket-based authentication. , 2008, , .		13
112	AAC-OT: Accountable Oblivious Transfer With Access Control. IEEE Transactions on Information Forensics and Security, 2015, 10, 2502-2514.	4.5	13
113	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. IEEE Systems Journal, 2017, 11, 1018-1026.	2.9	13
114	Security of Grouping-Proof Authentication Protocol for Distributed RFID Systems. IEEE Wireless Communications Letters, 2018, 7, 254-257.	3.2	13
115	Privacy-Preserving Cloud Auditing with Multiple Uploaders. Lecture Notes in Computer Science, 2016, , 224-237.	1.0	13
116	Optimal Online/Offline Signature: How to Sign a Message without Online Computation. Lecture Notes in Computer Science, 2008, , 98-111.	1.0	12
117	Provably Secure Homomorphic Signcryption. Lecture Notes in Computer Science, 2017, , 349-360.	1.0	12
118	Witness-based searchable encryption. Information Sciences, 2018, 453, 364-378.	4.0	12
119	A Fair Electronic Cash Scheme. Lecture Notes in Computer Science, 2001, , 20-32.	1.0	12
120	Robust non-interactive oblivious transfer. IEEE Communications Letters, 2003, 7, 153-155.	2.5	11
121	Dynamic Trust Model for Federated Identity Management. , 2010, , .		11
122	Provably Secure Single Sign-on Scheme in Distributed Systems and Networks. , 2012, , .		11
123	Membership Encryption and Its Applications. Lecture Notes in Computer Science, 2013, , 219-234.	1.0	11
124	A New Public Remote Integrity Checking Scheme with User Privacy. Lecture Notes in Computer Science, 2015, , 377-394.	1.0	11
125	Comment on â€œSecure quantum private information retrieval using phase-encoded queriesâ€• Physical Review A, 2016, 94, .	1.0	11
126	Strongly leakage resilient authenticated key exchange, revisited. Designs, Codes, and Cryptography, 2019, 87, 2885-2911.	1.0	11

#	Article	IF	Citations
127	The generic construction of continuous leakage-resilient identity-based cryptosystems. Theoretical Computer Science, 2019, 772, 1-45.	0.5	11
128	A code-based signature scheme from the Lyubashevsky framework. Theoretical Computer Science, 2020, 835, 15-30.	0.5	11
129	Improved Identity-Based Online/Offline Encryption. Lecture Notes in Computer Science, 2015, , 160-173.	1.0	11
130	A Generic Construction of Identity-Based Online/Offline Signcryption. , 2008, , .		10
131	Two Quantum Protocols for Oblivious Set-member Decision Problem. Scientific Reports, 2015, 5, 15914.	1.6	10
132	Privacy-Preserving Proof of Storage for the Pay-As-You-Go Business Model. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 563-575.	3.7	10
133	Novel generic construction of leakage-resilient PKE scheme with CCA security. Designs, Codes, and Cryptography, 2021, 89, 1575-1614.	1.0	10
134	PBTrust: A Priority-Based Trust Model for Service Selection in General Service-Oriented Environments. , 2010, , .		9
135	Privacy-Preserving Authorized RFID Authentication Protocols. Lecture Notes in Computer Science, 2014, , 108-122.	1.0	9
136	Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. Quantum Information Processing, 2017, 16, 1.	1.0	9
137	Secure-channel free keyword search with authorization in manager-centric databases. Computers and Security, 2017, 69, 50-64.	4.0	9
138	Designated Verifier Proxy Re-signature for Deniable and Anonymous Wireless Communications. Wireless Personal Communications, 2017, 97, 3017-3030.	1.8	9
139	New Approach for Privacy-Aware Location-Based Service Communications. Wireless Personal Communications, 2018, 101, 1057-1073.	1.8	9
140	Provably Secure (Broadcast) Homomorphic Signcryption. International Journal of Foundations of Computer Science, 2019, 30, 511-529.	0.8	9
141	Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage. IEEE Access, 2020, 8, 104344-104356.	2.6	9
142	Privacy-Preserving Flexible Access Control for Encrypted Data in Internet of Things. IEEE Internet of Things Journal, 2021, 8, 14731-14745.	5.5	9
143	A resilient identity-based authenticated key exchange protocol. Security and Communication Networks, 2015, 8, 2279-2290.	1.0	8
144	Compact Anonymous Hierarchical Identity-Based Encryption with Constant Size Private Keys: TABLE 1.. Computer Journal, 2016, 59, 452-461.	1.5	8

#	Article	IF	Citations
145	Privacy-enhanced attribute-based private information retrieval. Information Sciences, 2018, 454-455, 275-291.	4.0	8
146	Authenticated Data Redaction With Accountability and Transparency. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 149-160.	3.7	8
147	Privacy-Preserving Reverse Nearest Neighbor Query Over Encrypted Spatial Data. IEEE Transactions on Services Computing, 2022, 15, 2954-2968.	3.2	8
148	Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud. Journal of Systems Architecture, 2022, 129, 102569.	2.5	8
149	Ad Hoc Group Signatures. Lecture Notes in Computer Science, 2006, , 120-135.	1.0	7
150	Towards a cryptographic treatment of publish/subscribe systems1. Journal of Computer Security, 2014, 22, 33-67.	0.5	7
151	Efficient E-coupon systems with strong user privacy. Telecommunication Systems, 2017, 64, 695-708.	1.6	7
152	Privacy-Preserving Yoking Proof with Key Exchange in the Three-Party Setting. Wireless Personal Communications, 2017, 94, 1017-1034.	1.8	7
153	Privacy-enhanced remote data integrity checking with updatable timestamp. Information Sciences, 2020, 527, 210-226.	4.0	7
154	A traceable and revocable multi-authority access control scheme with privacy preserving for mHealth. Journal of Systems Architecture, 2022, 130, 102654.	2.5	7
155	Case-Based Trust Evaluation from Provenance Information. , 2011, , .		6
156	A secure mobility support scheme for 6LoWPAN wireless sensor networks. Security and Communication Networks, 2014, 7, 641-652.	1.0	6
157	Identity based identification from algebraic coding theory. Theoretical Computer Science, 2014, 520, 51-61.	0.5	6
158	Vulnerabilities of an ECC-based RFID authentication scheme. Security and Communication Networks, 2015, 8, 3262-3270.	1.0	6
159	Identity-based quotable ring signature. Information Sciences, 2015, 321, 71-89.	4.0	6
160	Privacyâ€preserving data search and sharing protocol for social networks through wireless applications. Concurrency Computation Practice and Experience, 2017, 29, e3870.	1.4	6
161	Privacy-Preserving Mutual Authentication in RFID with Designated Readers. Wireless Personal Communications, 2017, 96, 4819-4845.	1.8	6
162	Policy-controlled signatures and their applications. Computer Standards and Interfaces, 2017, 50, 26-41.	3.8	6

#	Article	IF	Citations
163	Improving Privacy-Preserving CP-ABE with Hidden Access Policy. Lecture Notes in Computer Science, 2018, , 596-605.	1.0	6
164	Continuous leakage-resilient identity-based encryption with leakage amplification. Designs, Codes, and Cryptography, 2019, 87, 2061-2090.	1.0	6
165	Anonymous and Updatable Identity-Based Hash Proof System. IEEE Systems Journal, 2019, 13, 2818-2829.	2.9	6
166	Threshold privacy-preserving cloud auditing with multiple uploaders. International Journal of Information Security, 2019, 18, 321-331.	2.3	6
167	Distributed Ciphertext-Policy Attribute-Based Encryption With Enhanced Collusion Resilience and Privacy Preservation. IEEE Systems Journal, 2022, 16, 735-746.	2.9	6
168	Hierarchical Identity-Based Online/Offline Encryption. , 2008, , .		5
169	Secure Mobile Agents with Designated Hosts. , 2009, , .		5
170	Optimistic Fair Exchange with Strong Resolution-Ambiguity. IEEE Journal on Selected Areas in Communications, 2011, 29, 1491-1502.	9.7	5
171	Efficient oblivious transfers with access control. Computers and Mathematics With Applications, 2012, 63, 827-837.	1.4	5
172	Comments on â€œAccountable and Privacy-Enhanced Access Control in Wireless Sensor Networksâ€• IEEE Transactions on Wireless Communications, 2016, 15, 3097-3099.	6.1	5
173	A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. Information Sciences, 2020, 516, 331-345.	4.0	5
174	Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. Theoretical Computer Science, 2020, 809, 277-295.	0.5	5
175	Secure and Privacy-Preserving Attribute-Based Sharing Framework in Vehicles Ad Hoc Networks. IEEE Access, 2020, 8, 116781-116795.	2.6	5
176	Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT. IEEE Transactions on Cloud Computing, 2023, 11, 217-228.	3.1	5
177	Secure and Privacy-Preserved Data Collection for IoT Wireless Sensors. IEEE Internet of Things Journal, 2021, 8, 17669-17677.	5.5	5
178	GTrust: An Innovated Trust Model for Group Services Selection in Web-Based Service-Oriented Environments. Lecture Notes in Computer Science, 2011, , 306-313.	1.0	5
179	An Efficient Certificateless Encryption Scheme in the Standard Model. , 2009, , .		4
180	Web Service Selection Based on Similarity Evaluation. , 2011, , .		4

#	Article	IF	Citations
181	Anonymous Proxy Signature with Restricted Traceability. , 2014, , .		4
182	Key management for Smart Grid based on asymmetric key-wrapping. International Journal of Computer Mathematics, 2015, 92, 498-512.	1.0	4
183	Multi-authority security framework for scalable EHR systems. International Journal of Medical Engineering and Informatics, 2016, 8, 390.	0.2	4
184	Efficient dynamic threshold identity-based encryption with constant-size ciphertext. Theoretical Computer Science, 2016, 609, 49-59.	0.5	4
185	Trust-based group services selection in web-based service-oriented environments. World Wide Web, 2016, 19, 807-832.	2.7	4
186	Efficient k-out-of-n oblivious transfer scheme with the ideal communication cost. Theoretical Computer Science, 2018, 714, 15-26.	0.5	4
187	Top-Level Secure Certificateless Signature Against Malicious-But-Passive KGC. IEEE Access, 2019, 7, 112870-112878.	2.6	4
188	ACE with Compact Ciphertext Size and Decentralized Sanitizers. International Journal of Foundations of Computer Science, 2019, 30, 531-549.	0.8	4
189	Novel updatable identity-based hash proof system and its applications. Theoretical Computer Science, 2020, 804, 1-28.	0.5	4
190	Efficient and secure image authentication with robustness and versatility. Science China Information Sciences, 2020, 63, 1.	2.7	4
191	Bidirectional and Malleable Proof-of-Ownership for Large File in Cloud Storage. IEEE Transactions on Cloud Computing, 2022, 10, 2351-2365.	3.1	4
192	Server-Aided Public Key Generation Protocols on Low-power Devices for Ad-hoc Networks. , 2006, , .		3
193	Multi-identity management for identity-based cryptography. Journal of Discrete Mathematical Sciences and Cryptography, 2008, 11, 639-672.	0.5	3
194	Efficient RFID Authentication Scheme for Supply Chain Applications. , 2010, , .		3
195	Advanced computer mathematics based cryptography and security technologies. International Journal of Computer Mathematics, 2013, 90, 2512-2514.	1.0	3
196	Public-Key Encryption Resilient against Linear Related-Key Attacks Revisited. , 2014, , .		3
197	Relations between robustness and RKA security under public-key encryption. Theoretical Computer Science, 2016, 628, 78-91.	0.5	3
198	A New Revocable and Re-Delegable Proxy Signature and Its Application. Journal of Computer Science and Technology, 2018, 33, 380-399.	0.9	3

#	Article	IF	Citations
199	Strong Identity-Based Proxy Signature Schemes, Revisited. Wireless Communications and Mobile Computing, 2018, 2018, 1-11.	0.8	3
200	Secure Data Sharing With Lightweight Computation in E-Health. IEEE Access, 2020, 8, 209630-209643.	2.6	3
201	An improved Durandal signature scheme. Science China Information Sciences, 2020, 63, 1.	2.7	3
202	Privacy-Aware Image Authentication from Cryptographic Primitives. Computer Journal, 2021, 64, 1178-1192.	1.5	3
203	Universal Designated Verifier Signatures with Threshold-Signers. Lecture Notes in Computer Science, 2009, , 89-109.	1.0	3
204	HUCDO. ACM Transactions on Cyber-Physical Systems, 2020, 4, 1-23.	1.9	3
205	Redactable Blockchain-Enabled Hierarchical Access Control Framework for Data Sharing in Electronic Medical Records. IEEE Systems Journal, 2023, 17, 1962-1973.	2.9	3
206	Privacy-Enhanced Internet Storage. , 0, , .		2
207	Secure mobile agents with controlled resources. Concurrency Computation Practice and Experience, 2011, 23, 1348-1366.	1.4	2
208	Short Signatures with a Tighter Security Reduction Without Random Oracles. Computer Journal, 2011, 54, 513-524.	1.5	2
209	New constructions of OSBE schemes and their applications in oblivious access control. International Journal of Information Security, 2012, 11, 389-401.	2.3	2
210	Security pitfalls of an efficient threshold proxy signature scheme for mobile agents. Information Processing Letters, 2014, 114, 5-8.	0.4	2
211	An <scp>IPv6</scp>â€based mobility framework for urban vehicular networks. International Journal of Network Management, 2015, 25, 141-158.	1.4	2
212	Further ideal multipartite access structures from integer polymatroids. Science China Information Sciences, 2015, 58, 1-13.	2.7	2
213	Loss-Tolerant Bundle Fragment Authentication for Space-Based DTNs. IEEE Transactions on Dependable and Secure Computing, 2015, 12, 615-625.	3.7	2
214	A Novel Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Anonymous Key Generation. Lecture Notes in Computer Science, 2018, , 435-446.	1.0	2
215	Efficient Traceable Oblivious Transfer and Its Applications. Lecture Notes in Computer Science, 2018, , 610-621.	1.0	2
216	Policy controlled system with anonymity. Theoretical Computer Science, 2018, 745, 87-113.	0.5	2

#	Article	IF	Citations
217	Unlinkable and Revocable Secret Handshake. Computer Journal, 2021, 64, 1303-1314.	1.5	2
218	Controllable software licensing system for sub-licensing. Journal of Information Security and Applications, 2022, 64, 103061.	1.8	2
219	Structured encryption for knowledge graphs. Information Sciences, 2022, 605, 43-70.	4.0	2
220	A Scalable Multi-service Group Key Management Scheme. , 2006, , .		1
221	SEFAP: An Email System for Anti-Phishing. , 2007, , .		1
222	Constructing an Authentication Token to Access External Services in Service Aggregation. , 2010, , .		1
223	Privacy preserving protocol for service aggregation in cloud computing. Software - Practice and Experience, 2012, 42, 467-483.	2.5	1
224	Identity-Based Mediated RSA Revisited. , 2013, , .		1
225	Fully Secure Hierarchical Inner Product Encryption for Privacy Preserving Keyword Searching in Cloud. , 2015, , .		1
226	Generalized closest substring encryption. Designs, Codes, and Cryptography, 2016, 80, 103-124.	1.0	1
227	A Generic Table Recomputation-Based Higher-Order Masking. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 36, 1779-1789.	1.9	1
228	Black-Box Accountable Authority Identity-Based Revocation System. Computer Journal, 2020, 63, 525-535.	1.5	1
229	Trust Negotiation with Trust Parameters. , 2006, , .		0
230	A New Secure Data Forwarding Protocol with Fault Detection for Wireless Ad Hoc Networks. , 2007, , .		0
231	The Acceptance of a Clinical IT Innovation by the Care Givers in Residential Aged Care 11-Weeks After the Software Implementation in Australia. , 2007, , .		0
232	Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacryptâ€™2004. Journal of Computer Science and Technology, 2007, 22, 71-74.	0.9	0
233	Short Group Signatures Without Random Oracles. Journal of Computer Science and Technology, 2007, 22, 805-821.	0.9	0
234	Further Analysis of a Practical Hierarchical Identity-Based Encryption Scheme. IEICE Transactions on Information and Systems, 2012, E95.D, 1690-1693.	0.4	0

#	Article	IF	Citations
235	Efficient and secure stored-value cards with leakage resilience. Computers and Electrical Engineering, 2012, 38, 370-380.	3.0	0
236	Verifiable and Anonymous Encryption in Asymmetric Bilinear Maps. , 2013, , .		0
237	Attribute Based Service Customization and Selection. , 2014, , .		0
238	Message from the Guest Editors. International Journal of Information Security, 2016, 15, 223-224.	2.3	0
239	A new generic construction of anonymous designated confirmer signature for privacy-preserving fair exchange. International Journal of Computer Mathematics, 2017, 94, 946-961.	1.0	0
240	Privacy-Preserving Data Packet Filtering Protocol with Source IP Authentication. Wireless Personal Communications, 2017, 95, 3509-3537.	1.8	0
241	Publicly verifiable secure communication with user and data privacy. Personal and Ubiquitous Computing, 2019, , 1.	1.9	0
242	On the Security of Symmetric Encryption Against Mass Surveillance. IEEE Access, 2020, 8, 175625-175636.	2.6	0
243	BA2Pâ€‰:â€‰Bidirectional and Anonymous Auction Protocol with Dispute-Freeness. Security and Communication Networks, 2021, 2021, 1-12.	1.0	0
244	Concurrent Signatures without a Conventional Keystone. , 2008, , .		0
245	Identity-Based Encryption With Continuous Leakage-Resilient CCA Security From Static Complexity Assumption. Computer Journal, 2023, 66, 924-940.	1.5	0
246	Secure and Efficient General Circuits Attribute-Based Access Control in Cloud Computing. IEEE Systems Journal, 2022, , 1-11.	2.9	0