Willy Susilo

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/3143554/publications.pdf

Version: 2024-02-01

627 papers	14,220 citations	24978 57 h-index	43802 91 g-index

653 all docs	653 docs citations	653 times ranked	5683 citing authors

#	Article	IF	Citations
1	Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage. IEEE Transactions on Information Forensics and Security, 2017, 12, 767-778.	4.5	342
2	An Efficient Signature Scheme from Bilinear Pairings and Its Applications. Lecture Notes in Computer Science, 2004, , 277-290.	1.0	313
3	An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data. IEEE Transactions on Information Forensics and Security, 2017, 12, 2402-2415.	4.5	302
4	Public Key Encryption with Keyword Search Revisited. Lecture Notes in Computer Science, 2008, , 1249-1259.	1.0	268
5	Trapdoor security in a searchable public-key encryption scheme with a designated tester. Journal of Systems and Software, 2010, 83, 763-771.	3.3	235
6	Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 391-406.	3.7	230
7	Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2018, 13, 912-925.	4.5	196
8	Attribute-based signature and its applications. , 2010, , .		188
9	Public key encryption with keyword search secure against keyword guessing attacks without random oracle. Information Sciences, 2013, 238, 221-241.	4.0	175
10	On the Security of Certificateless Signature Schemes from Asiacrypt 2003. Lecture Notes in Computer Science, 2005, , 13-25.	1.0	174
11	Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1981-1992.	4.5	172
12	Certificateless Signature Revisited. , 2007, , 308-322.		169
13	Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 72-83.	3.7	165
14	Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. Information Sciences, 2018, 444, 72-88.	4.0	156
15	Certificateless Public Key Encryption Without Pairing. Lecture Notes in Computer Science, 2005, , 134-148.	1.0	148
16	Constant-Size Dynamic k-TAA. Lecture Notes in Computer Science, 2006, , 111-125.	1.0	148
17	CP-ABE With Constant-Size Keys for Lightweight Devices. IEEE Transactions on Information Forensics and Security, 2014, 9, 763-771.	4.5	133
18	Secure Message Communication Protocol Among Vehicles in Smart City. IEEE Transactions on Vehicular Technology, 2018, 67, 4359-4373.	3.9	131

#	Article	IF	Citations
19	A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Future Generation Computer Systems, 2015, 52, 95-108.	4.9	128
20	Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions. IEEE Transactions on Information Forensics and Security, 2016, 11, 35-45.	4.5	128
21	Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems, 2012, 23, 2150-2162.	4.0	126
22	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
23	Efficient Fair Conditional Payments for Outsourcing Computations. IEEE Transactions on Information Forensics and Security, 2012, 7, 1687-1694.	4.5	112
24	Blockchain-based fair payment smart contract for public cloud storage auditing. Information Sciences, 2020, 519, 348-362.	4.0	111
25	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. IEEE Internet of Things Journal, 2020, 7, 10660-10672.	5.5	109
26	Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. Lecture Notes in Computer Science, 2005, , 380-397.	1.0	107
27	Improvements on an authentication scheme for vehicular sensor networks. Expert Systems With Applications, 2014, 41, 2559-2564.	4.4	106
28	Asymmetric Group Key Agreement. Lecture Notes in Computer Science, 2009, , 153-170.	1.0	106
29	Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies. IEEE Network, 2019, 33, 111-117.	4.9	104
30	Secure searchable public key encryption scheme against keyword guessing attacks. IEICE Electronics Express, 2009, 6, 237-243.	0.3	103
31	Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, 2016, 62, 85-91.	4.9	101
32	Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. Lecture Notes in Computer Science, 2003, , 191-204.	1.0	99
33	Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. Future Generation Computer Systems, 2018, 78, 720-729.	4.9	94
34	An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing. Lecture Notes in Computer Science, 2014, , 257-272.	1.0	92
35	A Ciphertext-Policy Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security. , 2013, , .		85
36	A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing. IEEE Transactions on Information Forensics and Security, 2014, 9, 1667-1680.	4.5	85

#	Article	IF	Citations
37	Improved searchable public key encryption with designated tester. , 2009, , .		83
38	Identity-based data storage in cloud computing. Future Generation Computer Systems, 2013, 29, 673-681.	4.9	83
39	Identity-Based Strong Designated Verifier Signature Schemes. Lecture Notes in Computer Science, 2004, , 313-324.	1.0	82
40	Designated-server identity-based authenticated encryption with keyword search for encrypted emails. Information Sciences, 2019, 481, 330-343.	4.0	82
41	Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1578-1589.	4.5	81
42	Blockchain-based public auditing and secure deduplication with fair arbitration. Information Sciences, 2020, 541, 409-425.	4.0	78
43	Secure and Efficient Cloud Data Deduplication With Randomized Tag. IEEE Transactions on Information Forensics and Security, 2017, 12, 532-543.	4.5	76
44	Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 2018, 14, 3712-3723.	7.2	76
45	Personal Health Record Systems and Their Security Protection. Journal of Medical Systems, 2006, 30, 309-315.	2.2	73
46	Certificateless Signatures: New Schemes and Security Models. Computer Journal, 2012, 55, 457-474.	1.5	72
47	A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks. Wireless Personal Communications, 2013, 73, 993-1004.	1.8	70
48	A New Payment System for Enhancing Location Privacy of Electric Vehicles. IEEE Transactions on Vehicular Technology, 2014, 63, 3-18.	3.9	70
49	Linkable Ring Signature with Unconditional Anonymity. IEEE Transactions on Knowledge and Data Engineering, 2014, 26, 157-165.	4.0	68
50	Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 679-691.	3.7	65
51	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
52	Efficient algorithms for secure outsourcing of bilinear pairings. Theoretical Computer Science, 2015, 562, 112-121.	0.5	64
53	Metamorphic Testing for Cybersecurity. Computer, 2016, 49, 48-55.	1.2	64
54	Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage. IEEE Transactions on Emerging Topics in Computing, 2020, 8, 377-390.	3.2	64

#	Article	IF	Citations
55	Secure Keyword Search and Data Sharing Mechanism for Cloud Computing. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	3.7	63
56	Strongly secure certificateless short signatures. Journal of Systems and Software, 2012, 85, 1409-1417.	3.3	62
57	Identity-based chameleon hashing and signatures without key exposure. Information Sciences, 2014, 265, 198-210.	4.0	62
58	Revocable Attribute-Based Encryption With Data Integrity in Clouds. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2864-2872.	3.7	62
59	Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems. Lecture Notes in Computer Science, 2009, , 295-308.	1.0	61
60	A general framework for secure sharing of personal health records in cloud system. Journal of Computer and System Sciences, 2017, 90, 46-62.	0.9	60
61	A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. IEEE Transactions on Information Forensics and Security, 2015, 10, 1193-1206.	4.5	59
62	Blockchain-Based Dynamic Provable Data Possession for Smart Cities. IEEE Internet of Things Journal, 2020, 7, 4143-4154.	5.5	59
63	Efficient Generic On-Line/Off-Line Signatures Without Key Exposure. Lecture Notes in Computer Science, 2007, , 18-30.	1.0	59
64	A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks. IEEE Transactions on Vehicular Technology, 2018, 67, 5409-5423.	3.9	58
65	Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theoretical Computer Science, 2013, 469, 1-14.	0.5	57
66	Secure sharing and searching for real-time video data in mobile cloud. IEEE Network, 2015, 29, 46-50.	4.9	57
67	Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 2016, 65, 1992-2004.	2.4	56
68	On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search. Lecture Notes in Computer Science, 2006, , 217-232.	1.0	55
69	Certificate-Based Signature: Security Model and Efficient Construction. Lecture Notes in Computer Science, 2007, , 110-125.	1.0	54
70	Adaptively Secure Identity-Based Broadcast Encryption With a Constant-Sized Ciphertext. IEEE Transactions on Information Forensics and Security, 2015, 10, 679-693.	4.5	54
71	Perfect Concurrent Signature Schemes. Lecture Notes in Computer Science, 2004, , 14-26.	1.0	52
72	Short Linkable Ring Signatures Revisited. Lecture Notes in Computer Science, 2006, , 101-115.	1.0	51

#	Article	IF	Citations
73	A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle. Lecture Notes in Computer Science, 2009, , 248-258.	1.0	50
74	A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 119-130.	3.7	50
75	Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems. IEEE Transactions on Parallel and Distributed Systems, 2021, 32, 561-574.	4.0	50
76	A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives. Health Information Management Journal, 2015, 44, 23-38.	0.9	49
77	A Verifiable and Fair Attribute-Based Proxy Re-Encryption Scheme for Data Sharing in Clouds. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2907-2919.	3.7	49
78	Revocable Ring Signature. Journal of Computer Science and Technology, 2007, 22, 785-794.	0.9	48
79	Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theoretical Computer Science, 2012, 462, 39-58.	0.5	48
80	Interactive three-dimensional visualization of network intrusion detection data for machine learning. Future Generation Computer Systems, 2020, 102, 292-306.	4.9	48
81	New constructions of fuzzy identity-based encryption. , 2007, , .		47
82	Efficient generic on-line/off-line (threshold) signatures without key exposure. Information Sciences, 2008, 178, 4192-4203.	4.0	47
83	Certificate Based (Linkable) Ring Signature. , 2007, , 79-92.		46
84	Generating Searchable Public-Key Ciphertexts With Hidden Structures for Fast Keyword Search. IEEE Transactions on Information Forensics and Security, 2015, 10, 1993-2006.	4.5	45
85	Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure. Personal and Ubiquitous Computing, 2018, 22, 55-67.	1.9	45
86	Proxy Signature Without Random Oracles. Lecture Notes in Computer Science, 2006, , 473-484.	1.0	44
87	<inline-formula><tex-math>k</tex-math><alternatives> <inline-graphic xlink:type="simple" xlink:href="huang-ieq1-2366741.gif"/></alternatives></inline-formula>-Times Attribute-Based Anonymous Access Control for Cloud Computing. IEEE Transactions on Computers, 2015, 64, 2595-2608.	2.4	44
88	A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. Designs, Codes, and Cryptography, 2018, 86, 2587-2603.	1.0	44
89	Efficient Linkable and/or Threshold Ring Signature Without Random Oracles. Computer Journal, 2013, 56, 407-421.	1.5	41
90	Identity-Based Proxy Signature from Pairings. Lecture Notes in Computer Science, 2007, , 22-31.	1.0	41

#	Article	IF	Citations
91	Biometrics for Electronic Health Records. Journal of Medical Systems, 2010, 34, 975-983.	2.2	40
92	Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. International Journal of Information Security, 2011, 10, 373-385.	2.3	40
93	RS-HABE: Revocable-storage and Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	40
94	Ambiguous Optimistic Fair Exchange. Lecture Notes in Computer Science, 2008, , 74-89.	1.0	40
95	Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications, 2013, 36, 582-592.	5.8	39
96	Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption. IEEE Transactions on Information Forensics and Security, 2016, 11, 247-257.	4.5	39
97	Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing. Lecture Notes in Computer Science, 2016, , 409-425.	1.0	39
98	Online/Offline Provable Data Possession. IEEE Transactions on Information Forensics and Security, 2017, 12, 1182-1194.	4.5	37
99	Efficient Optimistic Fair Exchange Secure in the Multi-user Setting and Chosen-Key Model without Random Oracles. Lecture Notes in Computer Science, 2008, , 106-120.	1.0	37
100	Certificate-Based Signature Schemes without Pairings or Random Oracles. Lecture Notes in Computer Science, 2008, , 285-297.	1.0	37
101	RFID Privacy Models Revisited. Lecture Notes in Computer Science, 2008, , 251-266.	1.0	37
102	On the security of auditing mechanisms for secure cloud storage. Future Generation Computer Systems, 2014, 30, 127-132.	4.9	36
103	Practical Multi-Keyword and Boolean Search Over Encrypted E-mail in Cloud Server. IEEE Transactions on Services Computing, 2021, 14, 1877-1889.	3.2	36
104	A cloud-aided privacy-preserving multi-dimensional data comparison protocol. Information Sciences, 2021, 545, 739-752.	4.0	36
105	Privacy enhanced data outsourcing in the cloud. Journal of Network and Computer Applications, 2012, 35, 1367-1373.	5.8	35
106	Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature. Lecture Notes in Computer Science, 2006, , 364-378.	1.0	34
107	Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security. Lecture Notes in Computer Science, 2006, , 99-110.	1.0	34
108	Identity-based conditional proxy re-encryption with fine grain policy. Computer Standards and Interfaces, 2017, 52, 1-9.	3.8	34

#	Article	IF	Citations
109	Practical Anonymous Divisible E-Cash from Bounded Accumulators. Lecture Notes in Computer Science, 2008, , 287-301.	1.0	34
110	Fully Homomorphic Encryption Using Hidden Ideal Lattice. IEEE Transactions on Information Forensics and Security, 2013, 8, 2127-2137.	4.5	33
111	PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption. Lecture Notes in Computer Science, 2014, , 73-90.	1.0	33
112	Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards. Wireless Personal Communications, 2015, 80, 1747-1760.	1.8	33
113	Constructions of certificate-based signature secure against key replacement attacks*. Journal of Computer Security, 2010, 18, 421-449.	0.5	32
114	Identity-based strong designated verifier signature revisited. Journal of Systems and Software, 2011, 84, 120-129.	3.3	32
115	Blockchain-Based Secure Deduplication and Shared Auditing in Decentralized Storage. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3941-3954.	3.7	32
116	A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World. Lecture Notes in Computer Science, 2005, , 480-489.	1.0	32
117	Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions. Lecture Notes in Computer Science, 2016, , 844-876.	1.0	32
118	A Key-Policy Attribute-Based Proxy Re-Encryption Without Random Oracles: Table 1.. Computer Journal, 2016, 59, 970-982.	1.5	31
119	Generic Construction of (Identity-Based) Perfect Concurrent Signatures. Lecture Notes in Computer Science, 2005, , 194-206.	1.0	31
120	A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects. Computers and Security, 2022, 112, 102498.	4.0	31
121	How to construct identity-based signatures without the key escrow problem. International Journal of Information Security, 2010, 9, 297-311.	2.3	30
122	Efficient chameleon hash functions in the enhanced collision resistant model. Information Sciences, 2020, 510, 155-164.	4.0	30
123	Escrowed Linkability of Ring Signatures and Its Applications. Lecture Notes in Computer Science, 2006, , 175-192.	1.0	30
124	Efficient public key encryption with revocable keyword search. Security and Communication Networks, 2014, 7, 466-472.	1.0	29
125	Strong authenticated key exchange with auxiliary inputs. Designs, Codes, and Cryptography, 2017, 85, 145-173.	1.0	29
126	Authorized Equality Test on Identity-Based Ciphertexts for Secret Data Sharing via Cloud Storage. IEEE Access, 2019, 7, 25409-25421.	2.6	29

#	Article	IF	Citations
127	Designated Verifier Signature: Definition, Framework and New Constructions. Lecture Notes in Computer Science, 2007, , 1191-1200.	1.0	28
128	Certificateless threshold signature scheme from bilinear maps. Information Sciences, 2010, 180, 4714-4728.	4.0	28
129	An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing. Lecture Notes in Computer Science, 2014, , 448-461.	1.0	28
130	Enhancing Location Privacy for Electric Vehicles (at the Right time). Lecture Notes in Computer Science, 2012, , 397-414.	1.0	28
131	Non-interactive Deniable Ring Authentication. Lecture Notes in Computer Science, 2004, , 386-401.	1.0	27
132	Anonymous Conditional Proxy Re-encryption without Random Oracle. Lecture Notes in Computer Science, 2009, , 47-60.	1.0	27
133	Secure universal designated verifier signature without random oracles. International Journal of Information Security, 2008, 7, 171-183.	2.3	26
134	Constant-Size Dynamic k-Times Anonymous Authentication. IEEE Systems Journal, 2013, 7, 249-261.	2.9	26
135	A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme. IEEE Internet of Things Journal, 2020, 7, 3083-3093.	5.5	26
136	Privacy-Preserving federated learning in medical diagnosis with homomorphic re-Encryption. Computer Standards and Interfaces, 2022, 80, 103583.	3.8	26
137	Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a) Tj ETQq1 1 0.784314 rgBT /Overlock 10 Tf 50	1.0	26
138	Traceable and Retrievable Identity-Based Encryption. Lecture Notes in Computer Science, 2008, , 94-110.	1.0	26
139	Identity-Based Chameleon Hash Scheme without Key Exposure. Lecture Notes in Computer Science, 2010, , 200-215.	1.0	26
140	Functionalities of free and open electronic health record systems. International Journal of Technology Assessment in Health Care, 2010, 26, 382-389.	0.2	25
141	Interactive conditional proxy re-encryption with fine grain policy. Journal of Systems and Software, 2011, 84, 2293-2302.	3.3	25
142	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
143	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
144	Short (Identity-Based) Strong Designated Verifier Signature Schemes. Lecture Notes in Computer Science, 2006, , 214-225.	1.0	25

#	Article	IF	Citations
145	A Suite of Non-pairing ID-Based Threshold Ring Signature Schemes with Different Levels of Anonymity (Extended Abstract). Lecture Notes in Computer Science, 2010, , 166-183.	1.0	25
146	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
147	Provably secure server-aided verification signatures. Computers and Mathematics With Applications, 2011, 61, 1705-1723.	1.4	24
148	Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. Lecture Notes in Computer Science, 2016, , 223-239.	1.0	24
149	Recipient Revocable Identity-Based Broadcast Encryption. , 2016, , .		24
150	Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. IEEE Wireless Communications, 2021, 28, 63-69.	6.6	24
151	A robust smart cardâ€'based anonymous user authentication protocol for wireless communications. Security and Communication Networks, 2014, 7, 987-993.	1.0	23
152	Optimized Identity-Based Encryption from Bilinear Pairing for Lightweight Devices. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 211-220.	3.7	23
153	A QR Code Watermarking Approach Based on the DWT-DCT Technique. Lecture Notes in Computer Science, 2017, , 314-331.	1.0	23
154	Dual Access Control for Cloud-Based Data Storage and Sharing. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	3.7	23
155	Multi-party Concurrent Signatures. Lecture Notes in Computer Science, 2006, , 131-145.	1.0	23
156	A New Signature Scheme Without Random Oracles from Bilinear Pairings. Lecture Notes in Computer Science, 2006, , 67-80.	1.0	23
157	Identity-Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption. Lecture Notes in Computer Science, 2004, , 169-181.	1.0	22
158	A ciphertextâ€policy attributeâ€based proxy reâ€encryption scheme for data sharing in public clouds. Concurrency Computation Practice and Experience, 2015, 27, 2004-2027.	1.4	22
159	Publicly Verifiable Databases With All Efficient Updating Operations. IEEE Transactions on Knowledge and Data Engineering, 2021, 33, 3729-3740.	4.0	22
160	On the Security of Nominative Signatures. Lecture Notes in Computer Science, 2005, , 329-335.	1.0	22
161	Practical Compact E-Cash. , 2007, , 431-445.		22
162	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

#	Article	IF	Citations
163	Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes. Information Sciences, 2018, 429, 349-360.	4.0	21
164	A Two-Stage Classifier Approach for Network Intrusion Detection. Lecture Notes in Computer Science, 2018, , 329-340.	1.0	21
165	Cooperative Secret Sharing Using QR Codes and Symmetric Keys. Symmetry, 2018, 10, 95.	1.1	21
166	Privacy-Preserved Access Control for Cloud Computing. , 2011, , .		20
167	Strongly Leakage-Resilient Authenticated Key Exchange. Lecture Notes in Computer Science, 2016, , 19-36.	1.0	20
168	A generalized attack on RSA type cryptosystems. Theoretical Computer Science, 2017, 704, 74-81.	0.5	20
169	Fuzzy Extractors for Biometric Identification. , 2017, , .		20
170	EACSIP: Extendable Access Control System With Integrity Protection for Enhancing Collaboration in the Cloud. IEEE Transactions on Information Forensics and Security, 2017, 12, 3110-3122.	4.5	20
171	Universal designated verifier signature scheme with non-delegatability in the standard model. Information Sciences, 2019, 479, 321-334.	4.0	20
172	Efficient Certificateless Signcryption in the Standard Model: Revisiting Luo and Wanâ€™s Scheme from Wireless Personal Communications (2018). Computer Journal, 2019, 62, 1178-1193.	1.5	20
173	Short Designated Verifier Proxy Signature from Pairings. Lecture Notes in Computer Science, 2005, , 835-844.	1.0	20
174	Server-Aided Verification Signatures: Definitions and New Constructions. Lecture Notes in Computer Science, 2008, , 141-155.	1.0	20
175	Tripartite Concurrent Signatures. IFIP Advances in Information and Communication Technology, 2005, , 425-441.	0.5	19
176	Subset Membership Encryption and Its Applications to Oblivious Transfer. IEEE Transactions on Information Forensics and Security, 2014, 9, 1098-1107.	4.5	19
177	Are the most popular users always trustworthy? The case of Yelp. Electronic Commerce Research and Applications, 2016, 20, 30-41.	2.5	19
178	Cloud computing security and privacy: Standards and regulations. Computer Standards and Interfaces, 2017, 54, 1-2.	3.8	19
179	Publicly verifiable databases with efficient insertion/deletion operations. Journal of Computer and System Sciences, 2017, 86, 49-58.	0.9	19
180	Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. International Journal of Information Security, 2018, 17, 533-548.	2.3	19

#	Article	IF	Citations
181	Privacy-Preserving Certificateless Cloud Auditing with Multiple Users. Wireless Personal Communications, 2019, 106, 1161-1182.	1.8	19
182	Identity-Based Universal Designated Verifier Signatures. Lecture Notes in Computer Science, 2005, , 825-834.	1.0	19
183	Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length. Lecture Notes in Computer Science, 2007, , 367-391.	1.0	19
184	Practical RFID ownership transfer scheme. Journal of Computer Security, 2011, 19, 319-341.	0.5	18
185	On the Fault-Detection Capabilities of Adaptive Random Test Case Prioritization: Case Studies with Large Test Suites. , 2012, , .		18
186	On the security of text-based 3D CAPTCHAs. Computers and Security, 2014, 45, 84-99.	4.0	18
187	Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. Computer Journal, 2015, 58, 2778-2792.	1.5	18
188	Identifying malicious web domains using machine learning techniques with online credibility and performance data. , 2016, , .		18
189	PKE-MET: Public-Key Encryption With Multi-Ciphertext Equality Test in Cloud Computing. IEEE Transactions on Cloud Computing, 2022, 10, 1476-1488.	3.1	18
190	PPO-DFK: A Privacy-Preserving Optimization of Distributed Fractional Knapsack With Application in Secure Footballer Configurations. IEEE Systems Journal, 2021, 15, 759-770.	2.9	18
191	Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles. IEEE Transactions on Vehicular Technology, 2021, 70, 11338-11351.	3.9	18
192	New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing. Lecture Notes in Computer Science, 2009, , 321-336.	1.0	18
193	Breaking an Animated CAPTCHA Scheme. Lecture Notes in Computer Science, 2012, , 12-29.	1.0	18
194	A New and Efficient Fail-stop Signature Scheme. Computer Journal, 2000, 43, 430-437.	1.5	17
195	Security and Access of Health Research Data. Journal of Medical Systems, 2007, 31, 103-107.	2.2	17
196	Attribute-Based Oblivious Access Control. Computer Journal, 2012, 55, 1202-1215.	1.5	17
197	Provably secure proxy signature scheme from factorization. Mathematical and Computer Modelling, 2012, 55, 1160-1168.	2.0	17
198	Realizing Fully Secure Unrestricted ID-Based Ring Signature in the Standard Model Based on HIBE. IEEE Transactions on Information Forensics and Security, 2013, 8, 1909-1922.	4.5	17

#	Article	IF	Citations
199	Certificateless designated verifier signature revisited: achieving a concrete scheme in the standard model. International Journal of Information Security, 2019, 18, 619-635.	2.3	17
200	Certificateless aggregate signature scheme secure against fully chosen-key attacks. Information Sciences, 2020, 514, 288-301.	4.0	17
201	Bestie: Very Practical Searchable Encryption with Forward and Backward Security. Lecture Notes in Computer Science, 2021, , 3-23.	1.0	17
202	Universal Designated Verifier Signature Without Delegatability. Lecture Notes in Computer Science, 2006, , 479-498.	1.0	17
203	Identity-Based On-Line/Off-Line Signcryption. , 2008, , .		16
204	Provably Secure Identity Based Provable Data Possession. Lecture Notes in Computer Science, 2015, , 310-325.	1.0	16
205	Towards Multi-user Searchable Encryption Supporting Boolean Query and Fast Decryption. Lecture Notes in Computer Science, 2017, , 24-38.	1.0	16
206	Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2138-2148.	3.7	16
207	AniCAP: An Animated 3D CAPTCHA Scheme Based on Motion Parallax. Lecture Notes in Computer Science, 2011, , 255-271.	1.0	16
208	ROSE: Robust Searchable Encryption With Forward and Backward Security. IEEE Transactions on Information Forensics and Security, 2022, 17, 1115-1130.	4.5	16
209	A fast and flexible attribute-based searchable encryption scheme supporting multi-search mechanism in cloud computing. Computer Standards and Interfaces, 2022, 82, 103635.	3.8	16
210	Convertible identity-based anonymous designated ring signatures. International Journal of Security and Networks, 2006, 1, 218.	0.1	15
211	Mobile ad-hoc network key management with certificateless cryptography. , 2008, , .		15
212	Group-oriented fair exchange of signatures. Information Sciences, 2011, 181, 3267-3283.	4.0	15
213	A Generic Scheme of plaintext-checkable database encryption. Information Sciences, 2018, 429, 88-101.	4.0	15
214	PLC Code-Level Vulnerabilities. , 2018, , .		15
215	Introduction to Security Reduction. , 2018, , .		15
216	CAPTCHA Design and Security Issues. , 2019, , 69-92.		15

#	Article	IF	Citations
217	Private Set Intersection With Authorization Over Outsourced Encrypted Datasets. IEEE Transactions on Information Forensics and Security, 2021, 16, 4050-4062.	4.5	15
218	Collusion-resistant identity-based Proxy Re-encryption: Lattice-based constructions in Standard Model. Theoretical Computer Science, 2021, 871, 16-29.	0.5	15
219	Generic server-aided secure multi-party computation in cloud computing. Computer Standards and Interfaces, 2022, 79, 103552.	3.8	15
220	Ring Signature with Designated Linkability. Lecture Notes in Computer Science, 2006, , 104-119.	1.0	15
221	Lattice-Based IBE with Equality Test in Standard Model. Lecture Notes in Computer Science, 2019, , 19-40.	1.0	15
222	Deniable Ring Authentication Revisited. Lecture Notes in Computer Science, 2004, , 149-163.	1.0	15
223	Formal Definition and Construction of Nominative Signature. Lecture Notes in Computer Science, 2007, , 57-68.	1.0	15
224	Threshold ring signature without random oracles. , 2011, , .		14
225	Fully secure hidden vector encryption under standard assumptions. Information Sciences, 2013, 232, 188-207.	4.0	14
226	Leakage Resilient Authenticated Key Exchange Secure in the Auxiliary Input Model. Lecture Notes in Computer Science, 2013, , 204-217.	1.0	14
227	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
228	A Lattice-Based Public Key Encryption with Equality Test in Standard Model. Lecture Notes in Computer Science, 2019, , 138-155.	1.0	14
229	DO-RA: Data-oriented runtime attestation for IoT devices. Computers and Security, 2020, 97, 101945.	4.0	14
230	Short E-Cash. Lecture Notes in Computer Science, 2005, , 332-346.	1.0	14
231	Restricted Universal Designated Verifier Signature. Lecture Notes in Computer Science, 2006, , 874-882.	1.0	14
232	Efficient Dynamic Provable Data Possession with Public Verifiability and Data Privacy. Lecture Notes in Computer Science, 2015, , 395-412.	1.0	14
233	Token-Controlled Public Key Encryption. Lecture Notes in Computer Science, 2005, , 386-397.	1.0	14
234	Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext. Lecture Notes in Computer Science, 2012, , 609-626.	1.0	14

#	Article	IF	Citations
235	Attribute-Based Hierarchical Access Control With Extendable Policy. IEEE Transactions on Information Forensics and Security, 2022, 17, 1868-1883.	4.5	14
236	Securing wireless mesh networks with ticket-based authentication. , 2008, , .		13
237	A Provably Secure Construction of Certificate-Based Encryption from Certificateless Encryption. Computer Journal, 2012, 55, 1157-1168.	1.5	13
238	Hierarchical conditional proxy re-encryption. Computer Standards and Interfaces, 2012, 34, 380-389.	3.8	13
239	Server-aided signatures verification secure against collusion attack. Information Security Technical Report, 2013, 17, 46-57.	1.3	13
240	Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key. Lecture Notes in Computer Science, 2015, , 252-269.	1.0	13
241	AAC-OT: Accountable Oblivious Transfer With Access Control. IEEE Transactions on Information Forensics and Security, 2015, 10, 2502-2514.	4.5	13
242	Fine-grained information flow control using attributes. Information Sciences, 2019, 484, 167-182.	4.0	13
243	A Secure Cloud Data Sharing Protocol for Enterprise Supporting Hierarchical Keyword Search. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1532-1543.	3.7	13
244	Harnessing Policy Authenticity for Hidden Ciphertext Policy Attribute-Based Encryption. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1856-1870.	3.7	13
245	An Efficient Static Blind Ring Signature Scheme. Lecture Notes in Computer Science, 2006, , 410-423.	1.0	13
246	Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings. Lecture Notes in Computer Science, 2006, , 251-265.	1.0	13
247	Privacy-Preserving Cloud Auditing with Multiple Uploaders. Lecture Notes in Computer Science, 2016, , 224-237.	1.0	13
248	Multi-party Stand-Alone and Setup-Free Verifiably Committed Signatures. , 2007, , 134-149.		13
249	Sanitizable Signatures Revisited. Lecture Notes in Computer Science, 2008, , 80-97.	1.0	13
250	Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme. Lecture Notes in Computer Science, 2012, , 10-21.	1.0	13
251	Towards Enhanced Security for Certificateless Public-Key Authenticated Encryption with Keyword Search. Lecture Notes in Computer Science, 2019, , 113-129.	1.0	13
252	Cryptanalaysis of an EPCC1G2 Standard Compliant Ownership Transfer Scheme. Wireless Personal Communications, 2013, 72, 245-258.	1.8	12

#	Article	IF	Citations
253	A short IDâ€based proxy signature scheme. International Journal of Communication Systems, 2016, 29, 859-873.	1.6	12
254	Efficient Privacy-Preserving Charging Station Reservation System for Electric Vehicles. Computer Journal, 2016, 59, 1040-1053.	1.5	12
255	Witness-based searchable encryption. Information Sciences, 2018, 453, 364-378.	4.0	12
256	Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks. Journal of Information Security and Applications, 2018, 39, 31-40.	1.8	12
257	CCA-Secure Revocable Identity-Based Encryption With Ciphertext Evolution in the Cloud. IEEE Access, 2018, 6, 56977-56983.	2.6	12
258	Data Security Storage Model of the Internet of Things Based on Blockchain. Computer Systems Science and Engineering, 2021, 36, 213-224.	1.9	12
259	An efficient multivariate threshold ring signature scheme. Computer Standards and Interfaces, 2021, 74, 103489.	3.8	12
260	Broadcast Attacks against Lattice-Based Cryptosystems. Lecture Notes in Computer Science, 2009, , 456-472.	1.0	12
261	Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes. Journal of Networks, 2006, 1, .	0.4	12
262	(Convertible) Undeniable Signatures Without Random Oracles. Lecture Notes in Computer Science, 2007, , 83-97.	1.0	12
263	A Generic Construction of Dynamic Single Sign-on with Strong Security. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 181-198.	0.2	12
264	A new efficient optimistic fair exchange protocol without random oracles. International Journal of Information Security, 2012, 11, 53-63.	2.3	11
265	Membership Encryption and Its Applications. Lecture Notes in Computer Science, 2013, , 219-234.	1.0	11
266	Asymmetric Cross-cryptosystem Re-encryption Applicable to Efficient and Secure Mobile Access to Outsourced Data. , 2015, , .		11
267	Public Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy. Lecture Notes in Computer Science, 2016, , 389-405.	1.0	11
268	An efficient and provably secure RFID grouping proof protocol. , 2017, , .		11
269	Dynamic Provable Data Possession Protocols with Public Verifiability and Data Privacy. Lecture Notes in Computer Science, 2017, , 485-505.	1.0	11
270	Strongly leakage resilient authenticated key exchange, revisited. Designs, Codes, and Cryptography, 2019, 87, 2885-2911.	1.0	11

#	Article	IF	Citations
271	Leakage-resilient group signature: Definitions and constructions. Information Sciences, 2020, 509, 119-132.	4.0	11
272	Revocable identity-based encryption with server-aided ciphertext evolution. Theoretical Computer Science, 2020, 815, 11-24.	0.5	11
273	Attribute-based proxy re-signature from standard lattices and its applications. Computer Standards and Interfaces, 2021, 75, 103499.	3.8	11
274	Software Engineering for Internet of Things: The Practitioners' Perspective. IEEE Transactions on Software Engineering, 2022, 48, 2857-2878.	4.3	11
275	A New Improved AES S-box with Enhanced Properties. Lecture Notes in Computer Science, 2020, , 125-141.	1.0	11
276	P2OFE: Privacy-Preserving Optimistic Fair Exchange of Digital Signatures. Lecture Notes in Computer Science, 2014, , 367-384.	1.0	11
277	A CAPTCHA Scheme Based on the Identification of Character Locations. Lecture Notes in Computer Science, 2014, , 60-74.	1.0	11
278	Improved Identity-Based Online/Offline Encryption. Lecture Notes in Computer Science, 2015, , 160-173.	1.0	11
279	Authentication and Transaction Verification Using QR Codes with a Mobile Device. Lecture Notes in Computer Science, 2016, , 437-451.	1.0	11
280	A Digital Signature Scheme Based on CVP â€‰â̂ž. , 2008, , 288-307.		11
281	Ranking Attack Graphs with Graph Neural Networks. Lecture Notes in Computer Science, 2009, , 345-359.	1.0	11
282	On the Security of NOEKEON against Side Channel Cube Attacks. Lecture Notes in Computer Science, 2010, , 45-55.	1.0	11
283	A Generic Construction of Identity-Based Online/Offline Signcryption. , 2008, , .		10
284	Identity-Based Secure DistributedData Storage Schemes. IEEE Transactions on Computers, 2014, 63, 941-953.	2.4	10
285	A short identity-based proxy ring signature scheme from RSA. Computer Standards and Interfaces, 2015, 38, 144-151.	3.8	10
286	LLL for ideal lattices: re-evaluation of the security of Gentryâ€“Haleviâ€™s FHE scheme. Designs, Codes, and Cryptography, 2015, 76, 325-344.	1.0	10
287	Optimal Security Reductions for Unique Signatures: Bypassing Impossibilities with a Counterexample. Lecture Notes in Computer Science, 2017, , 517-547.	1.0	10
288	Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. Journal of Information Security and Applications, 2018, 40, 193-198.	1.8	10

#	Article	IF	Citations
289	Public Key Authenticated Encryption With Designated Equality Test and its Applications in Diagnostic Related Groups. IEEE Access, 2019, 7, 135999-136011.	2.6	10
290	Leakage-resilient ring signature schemes. Theoretical Computer Science, 2019, 759, 1-13.	0.5	10
291	Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. Theoretical Computer Science, 2020, 809, 73-87.	0.5	10
292	Ciphertext-policy attribute-based proxy re-encryption via constrained PRFs. Science China Information Sciences, 2021, 64, 1.	2.7	10
293	Lightweight Public Key Encryption With Equality Test Supporting Partial Authorization in Cloud Storage. Computer Journal, 2021, 64, 1226-1238.	1.5	10
294	Lattice-based signcryption with equality test in standard model. Computer Standards and Interfaces, 2021, 76, 103515.	3.8	10
295	Towards Efficient Fully Randomized Message-Locked Encryption. Lecture Notes in Computer Science, 2016, , 361-375.	1.0	10
296	A New Attack on Three Variants of the RSA Cryptosystem. Lecture Notes in Computer Science, 2016, , 258-268.	1.0	10
297	Proof-of-Knowledge of Representation of Committed Value and Its Applications. Lecture Notes in Computer Science, 2010, , 352-369.	1.0	10
298	STE3D-CAP: Stereoscopic 3D CAPTCHA. Lecture Notes in Computer Science, 2010, , 221-240.	1.0	10
299	Breaking a 3D-Based CAPTCHA Scheme. Lecture Notes in Computer Science, 2012, , 391-405.	1.0	10
300	Practical Post-Quantum Signature Schemes fromÂIsomorphism Problems ofÂTrilinear Forms. Lecture Notes in Computer Science, 2022, , 582-612.	1.0	10
301	Self-organised group key management for ad hoc networks. , 2006, , .		9
302	Compact sequential aggregate signatures. , 2007, , .		9
303	Short fail-stop signature scheme based on factorization and discrete logarithm assumptions. Theoretical Computer Science, 2009, 410, 736-744.	0.5	9
304	Efficient Designated Confirmer Signature and DCS-Based Ambiguous Optimistic Fair Exchange. IEEE Transactions on Information Forensics and Security, 2011, 6, 1233-1247.	4.5	9
305	Privacy-Preserving Authorized RFID Authentication Protocols. Lecture Notes in Computer Science, 2014, , 108-122.	1.0	9
306	Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance. Lecture Notes in Computer Science, 2016, , 477-494.	1.0	9

#	Article	IF	Citations
307	Identity-Based Broadcast Encryption with Outsourced Partial Decryption for Hybrid Security Models in Edge Computing. , 2019, , .		9
308	Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats. SN Applied Sciences, 2019, 1, 1.	1.5	9
309	Accountable identity-based encryption with distributed private key generators. Information Sciences, 2019, 505, 352-366.	4.0	9
310	Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA. Computer Standards and Interfaces, 2021, 74, 103470.	3.8	9
311	P2DPI: Practical and Privacy-Preserving Deep Packet Inspection. , 2021, , .		9
312	Lattice-Based IBE with Equality Test Supporting Flexible Authorization in the Standard Model. Lecture Notes in Computer Science, 2020, , 624-643.	1.0	9
313	A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange. Lecture Notes in Computer Science, 2010, , 41-61.	1.0	9
314	Enhanced Target Collision Resistant Hash Functions Revisited. Lecture Notes in Computer Science, 2009, , 327-344.	1.0	9
315	Universal Designated Multi Verifier Signature Schemes. , 0, , .		8
316	Identity-based anonymous designated ring signatures. , 2006, , .		8
317	Efficient ID-Based Authenticated Group Key Agreement from Bilinear Pairings. Lecture Notes in Computer Science, 2006, , 521-532.	1.0	8
318	CAPTCHA Challenges for Massively Multiplayer Online Games: Mini-game CAPTCHAs. , 2010, , .		8
319	Extended cubes. , 2011, , .		8
320	The construction of ambiguous optimistic fair exchange from designated confirmer signature without random oracles. Information Sciences, 2013, 228, 222-238.	4.0	8
321	Shared RFID ownership transfer protocols. Computer Standards and Interfaces, 2015, 42, 95-104.	3.8	8
322	A resilient identity-based authenticated key exchange protocol. Security and Communication Networks, 2015, 8, 2279-2290.	1.0	8
323	Broadcast encryption with dealership. International Journal of Information Security, 2016, 15, 271-283.	2.3	8
324	Obfuscating Re-encryption Algorithm With Flexible and Controllable Multi-Hop on Untrusted Outsourcing Server. IEEE Access, 2017, 5, 26419-26434.	2.6	8

#	Article	IF	Citations
325	Privacy-enhanced attribute-based private information retrieval. Information Sciences, 2018, 454-455, 275-291.	4.0	8
326	A cost-effective software testing strategy employing online feedback information. Information Sciences, 2018, 422, 318-335.	4.0	8
327	A Secure and Authenticated Mobile Payment Protocol Against Off-Site Attack Strategy. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3564-3578.	3.7	8
328	New proofs of ownership for efficient data deduplicationÂin the adversarial conspiracy model. International Journal of Intelligent Systems, 2021, 36, 2753-2766.	3.3	8
329	Verifiable data streaming with efficient update for intelligent automation systems. International Journal of Intelligent Systems, 2022, 37, 1322-1338.	3.3	8
330	Secure Cloud Auditing with Efficient Ownership Transfer. Lecture Notes in Computer Science, 2020, , 611-631.	1.0	8
331	Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage. Lecture Notes in Computer Science, 2017, , 207-226.	1.0	8
332	Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility. Lecture Notes in Computer Science, 2007, , 25-39.	1.0	8
333	Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework). Lecture Notes in Computer Science, 2008, , 358-374.	1.0	8
334	A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack. Lecture Notes in Computer Science, 2009, , 143-155.	1.0	8
335	Further Observations on Optimistic Fair Exchange Protocols in the Multi-user Setting. Lecture Notes in Computer Science, 2010, , 124-141.	1.0	8
336	Efficient Non-interactive Range Proof. Lecture Notes in Computer Science, 2009, , 138-147.	1.0	8
337	Broadcast Authenticated Encryption withÂKeyword Search. Lecture Notes in Computer Science, 2021, , 193-213.	1.0	8
338	Chosen-Ciphertext Secure Homomorphic Proxy Re-Encryption. IEEE Transactions on Cloud Computing, 2022, 10, 2398-2408.	3.1	8
339	Puncturable Encryption: A Generic Construction from Delegatable Fully Key-Homomorphic Encryption. Lecture Notes in Computer Science, 2020, , 107-127.	1.0	8
340	Ad Hoc Group Signatures. Lecture Notes in Computer Science, 2006, , 120-135.	1.0	7
341	Securing electronic health records with broadcast encryption schemes. International Journal of Electronic Healthcare, 2006, 2, 175.	0.2	7
342	A Provable Secure ID-Based Explicit Authenticated Key Agreement Protocol Without Random Oracles. Journal of Computer Science and Technology, 2008, 23, 832-842.	0.9	7

#	Article	IF	Citations
343	Distributed Privacy-Preserving Secure Aggregation in Vehicular Communication. , 2011, , .		7
344	Server-aided signatures verification secure against collusion attack. , 2011, , .		7
345	Forward Secure Attribute-Based Signatures. Lecture Notes in Computer Science, 2012, , 167-177.	1.0	7
346	Towards a cryptographic treatment of publish/subscribe systems1. Journal of Computer Security, 2014, 22, 33-67.	0.5	7
347	A Visual One-Time Password Authentication Scheme Using Mobile Devices. Lecture Notes in Computer Science, 2015, , 243-257.	1.0	7
348	ABKSâ€CSC: attributeâ€based keyword search with constantâ€size ciphertexts. Security and Communication Networks, 2016, 9, 5003-5015.	1.0	7
349	Generally Hybrid Proxy Re-Encryption. , 2016, , .		7
350	An Efficient Key-Policy Attribute-Based Searchable Encryption in Prime-Order Groups. Lecture Notes in Computer Science, 2017, , 39-56.	1.0	7
351	A Multivariate Blind Ring Signature Scheme. Computer Journal, 2020, 63, 1194-1202.	1.5	7
352	Efficient Server-Aided Secure Two-Party Computation in Heterogeneous Mobile Cloud Computing. IEEE Transactions on Dependable and Secure Computing, 2021, , 1-1.	3.7	7
353	Lattice-Based HRA-secure Attribute-Based Proxy Re-Encryption in Standard Model. Lecture Notes in Computer Science, 2021, , 169-191.	1.0	7
354	Efficient Hidden Vector Encryption with Constant-Size Ciphertext. Lecture Notes in Computer Science, 2014, , 472-487.	1.0	7
355	Jhanwar-Baruaâ€™s Identity-Based Encryption Revisited. Lecture Notes in Computer Science, 2014, , 271-284.	1.0	7
356	Identity-Based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles. Lecture Notes in Computer Science, 2009, , 94-108.	1.0	7
357	Online/Offline Ring Signature Scheme. Lecture Notes in Computer Science, 2009, , 80-90.	1.0	7
358	Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships. Lecture Notes in Computer Science, 2010, , 192-211.	1.0	7
359	Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes. Lecture Notes in Computer Science, 2012, , 419-436.	1.0	7
360	Efficient Post-quantum Identity-based Encryption with Equality Test. , 2020, , .		7

#	Article	IF	Citations
361	Cryptanalysis on Two Certificateless Signature Schemes. International Journal of Computers, Communications and Control, 2014, 5, 586.	1.2	7
362	Relations among Privacy Notions for Signcryption and Key Invisible â€œSign-then-Encryptâ€• Lecture Notes in Computer Science, 2013, , 187-202.	1.0	7
363	Puncturable Proxy Re-Encryption Supporting to Group Messaging Service. Lecture Notes in Computer Science, 2019, , 215-233.	1.0	7
364	Inspecting TLS Anytime Anywhere: A New Approach to TLS Interception. , 2020, , .		7
365	Remark on self-certified group-oriented cryptosystem without combiner. Electronics Letters, 1999, 35, 1539.	0.5	6
366	Identity-Based Broadcasting. Lecture Notes in Computer Science, 2003, , 177-190.	1.0	6
367	Comparing and debugging firewall rule tables. IET Information Security, 2007, 1, 143.	1.1	6
368	Anonymous Single Sign-On Schemes Transformed from Group Signatures. , 2013, , .		6
369	(Strong) multidesignated verifiers signatures secure against rogue key attack. Concurrency Computation Practice and Experience, 2014, 26, 1574-1592.	1.4	6
370	Identity based identification from algebraic coding theory. Theoretical Computer Science, 2014, 520, 51-61.	0.5	6
371	Vulnerabilities of an ECC-based RFID authentication scheme. Security and Communication Networks, 2015, 8, 3262-3270.	1.0	6
372	File sharing in cloud computing using win stay lose shift strategy. International Journal of High Performance Computing and Networking, 2015, 8, 154.	0.4	6
373	Identity-based quotable ring signature. Information Sciences, 2015, 321, 71-89.	4.0	6
374	A Tag Based Encoding: An Efficient Encoding for Predicate Encryption in Prime Order Groups. Lecture Notes in Computer Science, 2016, , 3-22.	1.0	6
375	An Efficient KP-ABE with Short Ciphertexts in Prime OrderGroups under Standard Assumption. , 2017, , .		6
376	Privacy-Preserving Mutual Authentication in RFID with Designated Readers. Wireless Personal Communications, 2017, 96, 4819-4845.	1.8	6
377	Policy-controlled signatures and their applications. Computer Standards and Interfaces, 2017, 50, 26-41.	3.8	6
378	RFID Ownership Transfer with Positive Secrecy Capacity Channels. Sensors, 2017, 17, 53.	2.1	6

#	Article	IF	Citations
379	Dimensionality Reduction and Visualization of Network Intrusion Detection Data. Lecture Notes in Computer Science, 2019, , 441-455.	1.0	6
380	Threshold privacy-preserving cloud auditing with multiple uploaders. International Journal of Information Security, 2019, 18, 321-331.	2.3	6
381	Utilizing QR codes to verify the visual fidelity of image datasets for machine learning. Journal of Network and Computer Applications, 2021, 173, 102834.	5.8	6
382	Efficient and Privacy-Preserving Massive Data Processing for Smart Grids. IEEE Access, 2021, 9, 70616-70627.	2.6	6
383	Blockchain Based Multi-Authority Fine-Grained Access Control System With Flexible Revocation. IEEE Transactions on Services Computing, 2022, 15, 3143-3155.	3.2	6
384	Optimal Verifiable Data Streaming Protocol with Data Auditing. Lecture Notes in Computer Science, 2021, , 296-312.	1.0	6
385	Data Access Control in Cloud Computing: Flexible and Receiver Extendable. IEEE Transactions on Services Computing, 2022, 15, 2658-2670.	3.2	6
386	Efficient Semi-static Secure Broadcast Encryption Scheme. Lecture Notes in Computer Science, 2014, , 62-76.	1.0	6
387	Certificate-Based Signatures: New Definitions and a Generic Construction from Certificateless Signatures. Lecture Notes in Computer Science, 2009, , 99-114.	1.0	6
388	Improvement of Lattice-Based Cryptography Using CRT. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 275-282.	0.2	6
389	Improving BDD Cryptosystems in General Lattices. Lecture Notes in Computer Science, 2011, , 152-167.	1.0	6
390	Efficient Escrow-Free Identity-Based Signature. Lecture Notes in Computer Science, 2012, , 161-174.	1.0	6
391	Perfect Ambiguous Optimistic Fair Exchange. Lecture Notes in Computer Science, 2012, , 142-153.	1.0	6
392	Publicly Verifiable Privacy-Preserving Group Decryption. Lecture Notes in Computer Science, 2009, , 72-83.	1.0	6
393	Possibility and Impossibility Results for Receiver Selective Opening Secure PKE in the Multi-challenge Setting. Lecture Notes in Computer Science, 2020, , 191-220.	1.0	6
394	Secure Infectious Diseases Detection System With IoT-Based e-Health Platforms. IEEE Internet of Things Journal, 2022, 9, 22595-22607.	5.5	6
395	Identity-based trapdoor mercurial commitments and applications. Theoretical Computer Science, 2011, 412, 5498-5512.	0.5	5
396	Optimistic Fair Exchange with Strong Resolution-Ambiguity. IEEE Journal on Selected Areas in Communications, 2011, 29, 1491-1502.	9.7	5

#	Article	IF	Citations
397	Efficient oblivious transfers with access control. Computers and Mathematics With Applications, 2012, 63, 827-837.	1.4	5
398	Attribute-Based Data Transfer with Filtering Scheme in Cloud Computing. Computer Journal, 2014, 57, 579-591.	1.5	5
399	An Efficient Variant of Boneh-Gentry-Hamburgâ€™s Identity-Based Encryption Without Pairing. Lecture Notes in Computer Science, 2015, , 257-268.	1.0	5
400	Ambiguous optimistic fair exchange: Definition and constructions. Theoretical Computer Science, 2015, 562, 177-193.	0.5	5
401	Logarithmic size ring signatures without random oracles. IET Information Security, 2016, 10, 1-7.	1.1	5
402	A note on the strong authenticated key exchange with auxiliary inputs. Designs, Codes, and Cryptography, 2017, 85, 175-178.	1.0	5
403	Sequence aware functional encryption and its application in searchable encryption. Journal of Information Security and Applications, 2017, 35, 106-118.	1.8	5
404	Multiâ€designated verifiers signature schemes with threshold verifiability: generic pattern and a concrete scheme in the standard model. IET Information Security, 2019, 13, 459-468.	1.1	5
405	A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks. Sensors, 2019, 19, 2583.	2.1	5
406	A Blind Signature from Module Latices. , 2019, , .		5
407	An Anonymous Authentication System for Pay-As-You-Go Cloud Computing. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	3.7	5
408	Aggregatable Certificateless Designated Verifier Signature. IEEE Access, 2020, 8, 95019-95031.	2.6	5
409	Message-Locked Searchable Encryption: A New Versatile Tool for Secure Cloud Storage. IEEE Transactions on Services Computing, 2022, 15, 1664-1677.	3.2	5
410	Beating Random Test Case Prioritization. IEEE Transactions on Reliability, 2021, 70, 654-675.	3.5	5
411	A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations. Theoretical Computer Science, 2021, 885, 125-130.	0.5	5
412	On the Internal Structure of Alpha-MAC. Lecture Notes in Computer Science, 2006, , 271-285.	1.0	5
413	New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era. Lecture Notes in Computer Science, 2014, , 182-199.	1.0	5
414	(Strong) Multi-Designated Verifiers Signatures Secure against Rogue Key Attack. Lecture Notes in Computer Science, 2012, , 334-347.	1.0	5

#	Article	IF	Citations
415	A generalised bound for the Wiener attack on RSA. Journal of Information Security and Applications, 2020, 53, 102531.	1.8	5
416	Policy-Controlled Signatures. Lecture Notes in Computer Science, 2009, , 91-106.	1.0	5
417	Fail-Stop Threshold Signature Schemes Based on Elliptic Curves. Lecture Notes in Computer Science, 1999, , 103-116.	1.0	5
418	A Blind Ring Signature Based on the Short Integer Solution Problem. Lecture Notes in Computer Science, 2020, , 92-111.	1.0	5
419	Efficient Unique Ring Signature forÂBlockchain Privacy Protection. Lecture Notes in Computer Science, 2021, , 391-407.	1.0	5
420	A model-driven approach to reengineering processes in cloud computing. Information and Software Technology, 2022, 144, 106795.	3.0	5
421	FH-CFI: Fine-grained hardware-assisted control flow integrity for ARM-based IoT devices. Computers and Security, 2022, 116, 102666.	4.0	5
422	Information security and privacy of health data. International Journal of Healthcare Technology and Management, 2006, 7, 492.	0.1	4
423	Designated group credentials. , 2006, , .		4
424	Securing personal health information access in mobile healthcare environment through short signature schemes. International Journal of Mobile Communications, 2007, 5, 215.	0.2	4
425	Improving Software Testing Cost-Effectiveness through Dynamic Partitioning. , 2009, , .		4
426	On the security of the identity-based encryption based on DHIES from ASIACCS 2010. , 2011, , .		4
427	Server-Aided Signature Verification for Lightweight Devices. Computer Journal, 2014, 57, 481-493.	1.5	4
428	Deniability and forward secrecy of one-round authenticated key exchange. Journal of Supercomputing, 2014, 67, 671-690.	2.4	4
429	How to protect privacy in Optimistic Fair Exchange of digital signatures. Information Sciences, 2015, 325, 300-315.	4.0	4
430	An Identity-Based Multi-Proxy Multi-Signature Scheme Without Bilinear Pairings and its Variants. Computer Journal, 2015, 58, 1021-1039.	1.5	4
431	Multi-authority security framework for scalable EHR systems. International Journal of Medical Engineering and Informatics, 2016, 8, 390.	0.2	4
432	Efficient dynamic threshold identity-based encryption with constant-size ciphertext. Theoretical Computer Science, 2016, 609, 49-59.	0.5	4

#	Article	IF	Citations
433	A 3D Approach for the Visualization of Network Intrusion Detection Data. , 2018, , .		4
434	Subversion in Practice: How to Efficiently Undermine Signatures. IEEE Access, 2019, 7, 68799-68811.	2.6	4
435	Improving the Security of the DRS Scheme with Uniformly Chosen Random Noise. Lecture Notes in Computer Science, 2019, , 119-137.	1.0	4
436	Identity-Based Linkable Ring Signatures From Lattices. IEEE Access, 2021, 9, 84739-84755.	2.6	4
437	Efficient Signcryption Without Random Oracles. Lecture Notes in Computer Science, 2006, , 449-458.	1.0	4
438	Identity-Based Unidirectional Proxy Re-encryption in Standard Model: A Lattice-Based Construction. Lecture Notes in Computer Science, 2020, , 245-257.	1.0	4
439	Achieving Mobility and Anonymity in IP-Based Networks. , 2007, , 60-79.		4
440	New Construction of Group Secret Handshakes Based on Pairings. Lecture Notes in Computer Science, 2007, , 16-30.	1.0	4
441	How to Prove Security of a Signature with a Tighter Security Reduction. Lecture Notes in Computer Science, 2009, , 90-103.	1.0	4
442	Towards a Cryptographic Treatment of Publish/Subscribe Systems. Lecture Notes in Computer Science, 2010, , 201-220.	1.0	4
443	Fault Analysis of the KATAN Family of Block Ciphers. Lecture Notes in Computer Science, 2012, , 319-336.	1.0	4
444	An Efficient Fail-Stop Signature Scheme Based on Factorization. Lecture Notes in Computer Science, 2003, , 62-74.	1.0	4
445	X2BT Trusted Reputation System: A Robust Mechanism for P2P Networks. Lecture Notes in Computer Science, 2006, , 364-380.	1.0	4
446	Analysis of Property-Preservation Capabilities of the ROX and ESh Hash Domain Extenders. Lecture Notes in Computer Science, 2009, , 153-170.	1.0	4
447	How to Construct Identity-Based Signatures without the Key Escrow Problem. Lecture Notes in Computer Science, 2010, , 286-301.	1.0	4
448	Puncturable Identity-Based Encryption from Lattices. Lecture Notes in Computer Science, 2021, , 571-589.	1.0	4
449	Secure and Efficient Communication in VANETs Using Level-Based Access Control. Wireless Communications and Mobile Computing, 2022, 2022, 1-19.	0.8	4
450	Lattice-based public-key encryption with equality test supporting flexible authorization in standard model. Theoretical Computer Science, 2022, 929, 124-139.	0.5	4

#	Article	IF	Citations
451	Key Management for Secure Multicast with Dynamic Controller. Lecture Notes in Computer Science, 2000, , 178-190.	1.0	3
452	Provably secure fail-stop signature schemes based on RSA. International Journal of Wireless and Mobile Computing, 2005, 1, 53.	0.1	3
453	Efficient Trapdoor-Based Client Puzzle Against DoS Attacks. , 2010, , 229-249.		3
454	A framework for privacy policy management in service aggregation. , 2010, , .		3
455	Self-certified ring signatures. , 2011, , .		3
456	Privacy-preserving encryption scheme using DNA parentage test. Theoretical Computer Science, 2015, 580, 1-13.	0.5	3
457	A provably secure identityâ€based proxy ring signature based on RSA. Security and Communication Networks, 2015, 8, 1223-1236.	1.0	3
458	One-Round Strong Oblivious Signature-Based Envelope. Lecture Notes in Computer Science, 2016, , 3-20.	1.0	3
459	Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update. Lecture Notes in Computer Science, 2016, , 39-60.	1.0	3
460	SAKE: scalable authenticated key exchange for mobile eâ€health networks. Security and Communication Networks, 2016, 9, 2754-2765.	1.0	3
461	Editorial: Security and privacy protection vs sustainable development. Computers and Security, 2018, 76, 250-251.	4.0	3
462	Efficient Construction for Full Black-Box Accountable Authority Identity-Based Encryption. IEEE Access, 2019, 7, 25936-25947.	2.6	3
463	Optimally Efficient Secure Scalar Product With Applications in Cloud Computing. IEEE Access, 2019, 7, 42798-42815.	2.6	3
464	On the General Construction of Tightly Secure Identity-Based Signature Schemes. Computer Journal, 2020, 63, 1835-1848.	1.5	3
465	Group Encryption: Full Dynamicity, Message Filtering and Code-Based Instantiation. Lecture Notes in Computer Science, 2021, , 678-708.	1.0	3
466	Introduction to the Special Section on Artificial Intelligence Security: Adversarial Attack and Defense. IEEE Transactions on Network Science and Engineering, 2021, 8, 905-907.	4.1	3
467	Universal Designated Verifier Signatures with Threshold-Signers. Lecture Notes in Computer Science, 2009, , 89-109.	1.0	3
468	Short Generic Transformation to Strongly Unforgeable Signature in the Standard Model. Lecture Notes in Computer Science, 2010, , 168-181.	1.0	3

#	Article	IF	Citations
469	Efficient Online/Offline Signatures with Computational Leakage Resilience in Online Phase. Lecture Notes in Computer Science, 2011, , 455-470.	1.0	3
470	Lattice Reduction for Modular Knapsack. Lecture Notes in Computer Science, 2013, , 275-286.	1.0	3
471	Fail-Stop Signature for Long Messages (Extended Abstract). Lecture Notes in Computer Science, 2000, , 165-177.	1.0	3
472	A General Construction for Fail-Stop Signature using Authentication Codes. , 2001, , 343-356.		3
473	Secure AODV Routing Protocol Using One-Time Signature. Lecture Notes in Computer Science, 2005, , 288-297.	1.0	3
474	Transport Layer Identification of Skype Traffic. Lecture Notes in Computer Science, 2008, , 465-481.	1.0	3
475	Concurrent Signatures with Fully Negotiable Binding Control. Lecture Notes in Computer Science, 2011, , 170-187.	1.0	3
476	The Construction of Ambiguous Optimistic Fair Exchange from Designated Confirmer Signature without Random Oracles. Lecture Notes in Computer Science, 2012, , 120-137.	1.0	3
477	Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems. Communications in Computer and Information Science, 2017, , 3-13.	0.4	3
478	Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment. , 2019, , 1-22.		3
479	Ciphertext-Delegatable CP-ABE for a Dynamic Credential: A Modular Approach. Lecture Notes in Computer Science, 2019, , 3-20.	1.0	3
480	Short Principal Ideal Problem in multicubic fields. Journal of Mathematical Cryptology, 2020, 14, 359-392.	0.4	3
481	Trapdoor Delegation and HIBE from Middle-Product LWE in Standard Model. Lecture Notes in Computer Science, 2020, , 130-149.	1.0	3
482	A Generic Construction for Universally-Convertible Undeniable Signatures. , 2007, , 15-33.		3
483	Targeted Universal Adversarial Perturbations forÂAutomatic Speech Recognition. Lecture Notes in Computer Science, 2021, , 358-373.	1.0	3
484	Wildcarded identity-based encryption from lattices. Theoretical Computer Science, 2022, 902, 41-53.	0.5	3
485	Chosen-ciphertext lattice-based public key encryption with equality test in standard model. Theoretical Computer Science, 2022, 905, 31-53.	0.5	3
486	Privacy-preserving file sharing on cloud storage with certificateless signcryption. Theoretical Computer Science, 2022, 916, 1-21.	0.5	3

#	Article	IF	Citations
487	Attack on Han et al.â€™s ID-based confirmer (undeniable) signature at ACM-ECâ€™03. Applied Mathematics and Computation, 2005, 170, 1166-1169.	1.4	2
488	Efficient Partially Blind Signatures with Provable Security. Lecture Notes in Computer Science, 2007, , 1096-1105.	1.0	2
489	Is the Notion of Divisible On-Line/Off-Line Signatures Stronger than On-Line/Off-Line Signatures?. Lecture Notes in Computer Science, 2009, , 129-139.	1.0	2
490	Repeated Differential Properties of the AES-128 and AES-256 Key Schedules. , 2011, , .		2
491	Improving security of q-SDH based digital signatures. Journal of Systems and Software, 2011, 84, 1783-1790.	3.3	2
492	Short Signatures with a Tighter Security Reduction Without Random Oracles. Computer Journal, 2011, 54, 513-524.	1.5	2
493	New constructions of OSBE schemes and their applications in oblivious access control. International Journal of Information Security, 2012, 11, 389-401.	2.3	2
494	Secure Single Sign-On Schemes Constructed from Nominative Signatures. , 2013, , .		2
495	Security pitfalls of an efficient threshold proxy signature scheme for mobile agents. Information Processing Letters, 2014, 114, 5-8.	0.4	2
496	Attribute-based optimistic fair exchange: How to restrict brokers with policies. Theoretical Computer Science, 2014, 527, 83-96.	0.5	2
497	Protecting peer-to-peer-based massively multiplayer online games. International Journal of Computational Science and Engineering, 2015, 10, 293.	0.4	2
498	Anonymous Yoking-Group Proofs. , 2015, , .		2
499	Optimistic fair exchange in the enhanced chosen-key model. Theoretical Computer Science, 2015, 562, 57-74.	0.5	2
500	A semantic web vision for an intelligent community transport service brokering system. , 2016, , .		2
501	Faulty Instantiations of Threshold Ring Signature from Threshold Proof-of-Knowledge Protocol. Computer Journal, 2016, 59, 945-954.	1.5	2
502	Policy controlled system with anonymity. Theoretical Computer Science, 2018, 745, 87-113.	0.5	2
503	Generalized public-key cryptography with tight security. Information Sciences, 2019, 504, 561-577.	4.0	2
504	Enhancing Goldreich, Goldwasser and Haleviâ€™s scheme with intersecting lattices. Journal of Mathematical Cryptology, 2019, 13, 169-196.	0.4	2

#	Article	IF	Citations
505	Identity-based revocation system: Enhanced security model and scalable bounded IBRS construction with short parameters. Information Sciences, 2019, 472, 35-52.	4.0	2
506	An Efficient Postâ€quantum Identityâ€Based Signature. Chinese Journal of Electronics, 2021, 30, 238-248.	0.7	2
507	Non-Equivocation in Blockchain: Double-Authentication-Preventing Signatures Gone Contractual. , 2021, , .		2
508	An Adversary Aware and Intrusion Detection Aware Attack Model Ranking Scheme. Lecture Notes in Computer Science, 2007, , 65-86.	1.0	2
509	Threshold-Oriented Optimistic Fair Exchange. Lecture Notes in Computer Science, 2013, , 424-438.	1.0	2
510	Robust digital signature revisited. Theoretical Computer Science, 2020, 844, 87-96.	0.5	2
511	Threshold Fail-Stop Signature Schemes Based on Discrete Logarithm and Factorization. Lecture Notes in Computer Science, 2000, , 292-307.	1.0	2
512	Recursive Lattice Reduction. Lecture Notes in Computer Science, 2010, , 329-344.	1.0	2
513	Electronic Cash with Anonymous User Suspension. Lecture Notes in Computer Science, 2011, , 172-188.	1.0	2
514	Attribute-Based Signature with Message Recovery. Lecture Notes in Computer Science, 2014, , 433-447.	1.0	2
515	Foundations of Security Reduction. , 2018, , 29-146.		2
516	Using Freivaldsâ€™ Algorithm to Accelerate Lattice-Based Signature Verifications. Lecture Notes in Computer Science, 2019, , 401-412.	1.0	2
517	Functional signatures: new definition and constructions. Science China Information Sciences, 2021, 64, 1.	2.7	2
518	A Lattice-Based Certificateless Public Key Encryption with Equality Test in Standard Model. Lecture Notes in Computer Science, 2020, , 50-65.	1.0	2
519	QR Code Watermarking for Digital Images. Lecture Notes in Computer Science, 2020, , 25-37.	1.0	2
520	Efficient Anonymous Multi-group Broadcast Encryption. Lecture Notes in Computer Science, 2020, , 251-270.	1.0	2
521	A Five-Round Algebraic Property of the Advanced Encryption Standard. Lecture Notes in Computer Science, 2008, , 316-330.	1.0	2
522	Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits. Lecture Notes in Computer Science, 2021, , 42-53.	1.0	2

#	Article	IF	Citations
523	Generating Residue Number System Bases. , 2021, , .		2
524	SEFAP: An Email System for Anti-Phishing. , 2007, , .		1
525	A five-round algebraic property of AES and its application to the ALPHA-MAC. International Journal of Applied Cryptography, 2009, 1, 264.	0.4	1
526	Constructing an Authentication Token to Access External Services in Service Aggregation. , 2010, , .		1
527	Privacy preserving protocol for service aggregation in cloud computing. Software - Practice and Experience, 2012, 42, 467-483.	2.5	1
528	Secure RFID Ownership Transfer Protocols. Lecture Notes in Computer Science, 2013, , 189-203.	1.0	1
529	Privacy-Enhanced Keyword Search in Clouds. , 2013, , .		1
530	Identity-Based Mediated RSA Revisited. , 2013, , .		1
531	Revisiting Optimistic Fair Exchange Based on Ring Signatures. IEEE Transactions on Information Forensics and Security, 2014, 9, 1883-1892.	4.5	1
532	Collusion-Resistance in Optimistic Fair Exchange. IEEE Transactions on Information Forensics and Security, 2014, 9, 1227-1239.	4.5	1
533	Revisiting Security Against the Arbitrator in Optimistic Fair Exchange. Computer Journal, 2015, 58, 2665-2676.	1.5	1
534	Secure Delegation of Signing Power from Factorization. Computer Journal, 2015, 58, 867-877.	1.5	1
535	Anonymous Announcement System (AAS) for Electric Vehicle in VANETs. Computer Journal, 2016, , .	1.5	1
536	Solutions to the anti-piracy problem in oblivious transfer. Journal of Computer and System Sciences, 2016, 82, 466-476.	0.9	1
537	Generalized closest substring encryption. Designs, Codes, and Cryptography, 2016, 80, 103-124.	1.0	1
538	Securely Reinforcing Synchronization for Embedded Online Contests. Transactions on Embedded Computing Systems, 2017, 16, 1-21.	2.1	1
539	Covert QR Codes: How to Hide in the Crowd. Lecture Notes in Computer Science, 2017, , 678-693.	1.0	1
540	Threat Models for Analyzing PlausibleDeniability of Deniable File Systems. Software Networking, 2017, 2017, 241-264.	0.6	1

#	Article	IF	Citations
541	Functional encryption for computational hiding in prime order groups via pair encodings. Designs, Codes, and Cryptography, 2018, 86, 97-120.	1.0	1
542	Criteria-Based Encryption. Computer Journal, 2018, 61, 512-525.	1.5	1
543	PPFilter: Provider Privacy-aware Encrypted Filtering System. IEEE Transactions on Services Computing, 2018, , 1-1.	3.2	1
544	Leakage-Resilient Dual-Form Signatures. Computer Journal, 2018, 61, 1216-1227.	1.5	1
545	A System Model for Personalized Medication Management (MyMediMan)â€"The Consumersâ€™ Point of View. Information (Switzerland), 2018, 9, 69.	1.7	1
546	Keyword Attacks and Privacy Preserving in Public-Key-Based Searchable Encryption. , 2018, , 1-7.		1
547	Location Based Encryption. Lecture Notes in Computer Science, 2019, , 21-38.	1.0	1
548	Tightly Secure Public-Key Cryptographic Schemes from One-More Assumptions. Journal of Computer Science and Technology, 2019, 34, 1366-1379.	0.9	1
549	Black-Box Accountable Authority Identity-Based Revocation System. Computer Journal, 2020, 63, 525-535.	1.5	1
550	SyLPEnIoT: Symmetric Lightweight Predicate Encryption for Data Privacy Applications in IoT Environments. Lecture Notes in Computer Science, 2021, , 106-126.	1.0	1
551	Black-Box Audio Adversarial Example Generation Using Variational Autoencoder. Lecture Notes in Computer Science, 2021, , 142-160.	1.0	1
552	On Random-Oracle-Free Top-Level Secure Certificateless Signature Schemes. Computer Journal, 0, , .	1.5	1
553	Generic construction for tightly-secure signatures from discrete log. Theoretical Computer Science, 2021, 888, 13-21.	0.5	1
554	Mixed-protocol multi-party computation framework towards complex computation tasks with malicious security. Computer Standards and Interfaces, 2022, 80, 103570.	3.8	1
555	Password Protected Secret Sharing fromÂLattices. Lecture Notes in Computer Science, 2021, , 442-459.	1.0	1
556	Provably Secure Group Authentication in the Asynchronous Communication Model. Lecture Notes in Computer Science, 2020, , 324-340.	1.0	1
557	How to Balance Privacy with Authenticity. Lecture Notes in Computer Science, 2009, , 184-201.	1.0	1
558	Enhanced STE3D-CAP: A Novel 3D CAPTCHA Family. Lecture Notes in Computer Science, 2012, , 170-181.	1.0	1

#	Article	IF	Citations
559	Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction. Lecture Notes in Computer Science, 2016, , 745-776.	1.0	1
560	Deniable Partial Proxy Signatures. Lecture Notes in Computer Science, 2004, , 182-194.	1.0	1
561	On Securing RTP-Based Streaming Content with Firewalls. Lecture Notes in Computer Science, 2005, , 304-319.	1.0	1
562	Separable Identity-Based Deniable Authentication: Cryptographic Primitive for Fighting Phishing. Lecture Notes in Computer Science, 2006, , 68-80.	1.0	1
563	Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction. Lecture Notes in Computer Science, 2007, , 16-29.	1.0	1
564	Escrowed Deniable Identification Schemes. Communications in Computer and Information Science, 2009, , 234-241.	0.4	1
565	Privacy for Private Key in Signatures. Lecture Notes in Computer Science, 2009, , 84-95.	1.0	1
566	An Efficient Construction of Time-Selective Convertible Undeniable Signatures. Lecture Notes in Computer Science, 2011, , 355-371.	1.0	1
567	Secure Exchange of Electronic Health Records. , 2011, , 1-22.		1
568	Efficient Self-certified Signatures with Batch Verification. Lecture Notes in Computer Science, 2012, , 179-194.	1.0	1
569	Multi-Level Controlled Signature. Lecture Notes in Computer Science, 2012, , 96-110.	1.0	1
570	Generic Mediated Encryption. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2013, , 154-168.	0.2	1
571	Fair Multi-signature. Lecture Notes in Computer Science, 2015, , 244-256.	1.0	1
572	Mergeable and Revocable Identity-Based Encryption. Lecture Notes in Computer Science, 2017, , 147-167.	1.0	1
573	Improved Threat Models for the Security of Encrypted and Deniable File Systems. Lecture Notes in Electrical Engineering, 2018, , 223-230.	0.3	1
574	Improved Cryptanalysis of the KMOV Elliptic Curve Cryptosystem. Lecture Notes in Computer Science, 2019, , 206-221.	1.0	1
575	Concise Mercurial Subvector Commitments: Definitions andÂConstructions. Lecture Notes in Computer Science, 2021, , 353-371.	1.0	1
576	Towards Visualizing and Detecting Audio Adversarial Examples for Automatic Speech Recognition. Lecture Notes in Computer Science, 2021, , 531-549.	1.0	1

#	Article	IF	Citations
577	Hierarchical Identity-Based Signature in Polynomial Rings. Computer Journal, 2020, 63, 1490-1499.	1.5	1
578	Lattice-Based Group Encryption withÂFull Dynamicity andÂMessage Filtering Policy. Lecture Notes in Computer Science, 2021, , 156-186.	1.0	1
579	Trojan Attacks andÂDefense forÂSpeech Recognition. Communications in Computer and Information Science, 2022, , 195-210.	0.4	1
580	Functional Encryption for Pattern Matching with a Hidden String. Cryptography, 2022, 6, 1.	1.4	1
581	Optimal Tightness forÂChain-Based Unique Signatures. Lecture Notes in Computer Science, 2022, , 553-583.	1.0	1
582	Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacryptâ€™2004. Journal of Computer Science and Technology, 2007, 22, 71-74.	0.9	0
583	Short Group Signatures Without Random Oracles. Journal of Computer Science and Technology, 2007, 22, 805-821.	0.9	0
584	Fuzzy Identity-based Encryption: New and Efficient Schemes. , 2008, , .		0
585	Efficient lattice-based signature scheme. International Journal of Applied Cryptography, 2008, 1, 120.	0.4	0
586	Efficient and secure stored-value cards with leakage resilience. Computers and Electrical Engineering, 2012, 38, 370-380.	3.0	0
587	Two-Party (Blind) Ring Signatures and Their Applications. Lecture Notes in Computer Science, 2014, , 403-417.	1.0	0
588	Achieving fairness by sequential equilibrium in rational twoâ€party computation under incomplete information. Security and Communication Networks, 2015, 8, 3690-3700.	1.0	0
589	PEVTS: Privacy-Preserving Electric Vehicles Test-Bedding Scheme. , 2015, , .		0
590	Collusion-resistant convertible ring signature schemes. Science China Information Sciences, 2015, 58, 1-16.	2.7	0
591	Message from the Guest Editors. International Journal of Information Security, 2016, 15, 223-224.	2.3	0
592	Dirichlet product for boolean functions. Journal of Applied Mathematics and Computing, 2017, 55, 293-312.	1.2	0
593	The code for securing web applications. Journal of Information and Optimization Sciences, 2019, 40, 905-917.	0.2	0
594	A New Encoding Framework for Predicate Encryption with Non-linear Structures in Prime Order Groups. Lecture Notes in Computer Science, 2019, , 406-425.	1.0	0

#	Article	IF	Citations
595	Security, Privacy, and Trust for Cyberphysical-Social Systems. Security and Communication Networks, 2019, 2019, 1-2.	1.0	0
596	Message from the IEEE TrustCom 2019 Program Chairs. , 2019, , .		0
597	DABKE: Secure deniable attribute-based key exchange framework. Journal of Computer Security, 2019, 27, 259-275.	0.5	0
598	Concise ID-based mercurial functional commitments and applications to zero-knowledge sets. International Journal of Information Security, 2020, 19, 453-464.	2.3	0
599	A New Approach to Keep the Privacy Information of the Signer in a Digital Signature Scheme. Information (Switzerland), 2020, 11, 260.	1.7	0
600	A Noise Study of the PSW Signature Family: Patching DRS with Uniform Distribution â€. Information (Switzerland), 2020, 11, 133.	1.7	0
601	Efficient and Adaptive Procurement Protocol with Purchasing Privacy. IEEE Transactions on Services Computing, 2021, 14, 683-694.	3.2	0
602	Visual Analysis of Adversarial Examples in Machine Learning. , 2021, , 85-98.		0
603	On delegatability of MDVS schemes. Journal of Computer Virology and Hacking Techniques, 0, , 1.	1.6	0
604	Efficient maliciously secure two-party mixed-protocol framework for data-driven computation tasks. Computer Standards and Interfaces, 2022, 80, 103571.	3.8	0
605	Pattern Matching over Encrypted Data with a Short Ciphertext. Lecture Notes in Computer Science, 2021, , 132-143.	1.0	0
606	Secure Computation of Shared Secrets and Its Applications. Lecture Notes in Computer Science, 2021, , 119-131.	1.0	0
607	On Classifying Conference Key Distribution Protocols. Lecture Notes in Computer Science, 2001, , 51-59.	1.0	0
608	How to Construct Fail-Stop Confirmer Signature Schemes. Lecture Notes in Computer Science, 2001, , 435-444.	1.0	0
609	Zero-Knowledge Proof of Generalized Compact Knapsacks (or A Novel Identification/Signature) Tj ETQq1 1 0.784314 rgBT /Overlock 10	1.0	0
610	Privately Retrieve Data from Large Databases. Lecture Notes in Computer Science, 2006, , 367-378.	1.0	0
611	Efficient Authentication Schemes for AODV and DSR. , 2007, , 367-389.		0
612	Concurrent Signatures without a Conventional Keystone. , 2008, , .		0

#	Article	IF	Citations
613	Security Vulnerability of ID-Based Key Sharing Schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 2641-2643.	0.2	0
614	Differential Fault Analysis of LEX. Lecture Notes in Computer Science, 2010, , 55-72.	1.0	0
615	On Capabilities of Hash Domain Extenders to Preserve Enhanced Security Properties. Lecture Notes in Computer Science, 2012, , 288-299.	1.0	0
616	A Pre-computable Signature Scheme with Efficient Verification for RFID. Lecture Notes in Computer Science, 2012, , 1-16.	1.0	0
617	Towards Formalizing a Reputation System for Cheating Detection in Peer-to-Peer-Based Massively Multiplayer Online Games. Lecture Notes in Computer Science, 2012, , 291-304.	1.0	0
618	Secure Exchange of Electronic Health Records. , 2013, , 1059-1079.		0
619	Identity-Based Multisignature with Message Recovery. Lecture Notes in Computer Science, 2013, , 91-104.	1.0	0
620	Ideals of Largest Weight in Constructions Based on Directed Graphs. Bulletin of Mathematical Sciences and Applications, 0, 15, 8-16.	0.0	0
621	Protecting the Visual Fidelity of Machine Learning Datasets Using QR Codes. Lecture Notes in Computer Science, 2019, , 320-335.	1.0	0
622	Keyword Attacks and Privacy Preserving in Public-Key-Based Searchable Encryption. , 2019, , 1067-1073.		0
623	Forward-Secure Group Encryptions fromÂLattices. Lecture Notes in Computer Science, 2021, , 610-629.	1.0	0
624	Secure Exchange of Electronic Health Records. , 0, , 1403-1424.		0
625	Cryptanalysis of BGW Broadcast Encryption Schemes for DVD Content Protection. Lecture Notes in Computer Science, 2007, , 32-41.	1.0	0
626	Tight bound on NewHope failure probability. IEEE Transactions on Emerging Topics in Computing, 2022, , 1-1.	3.2	0
627	Securing Mobile Data Computing in Healthcare. , 0, , 1930-1939.		0