Yi Mu

List of Publications by Year in Descending Order

233 papers	3,407 citations	28 h-index	46 g-index
248 ext. papers	4,093 ext. citations	3.2 avg, IF	5.88 L-index

#	Paper	IF	Citations
233	Blockchain-based random auditor committee for integrity verification. *Future Generation Computer Systems*, **2022**, 131, 183-193	7.5	2
232	Secure and Efficient General Circuits Attribute-Based Access Control in Cloud Computing. *IEEE Systems Journal*, **2022**, 1-11	4.3	
231	Controllable software licensing system for sub-licensing. *Journal of Information Security and Applications*, **2022**, 64, 103061	3.5	0
230	Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud. *Journal of Systems Architecture*, **2022**, 102569	5.5	0
229	Secure Decentralized Attribute-Based Sharing of Personal Health Records with Blockchain. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	1
228	BA2P : Bidirectional and Anonymous Auction Protocol with Dispute-Freeness. *Security and Communication Networks*, **2021**, 2021, 1-12	1.9	
227	Novel generic construction of leakage-resilient PKE scheme with CCA security. *Designs, Codes, and Cryptography*, **2021**, 89, 1575	1.2	1
226	An Expressive Test-Decrypt-Verify Attribute-Based Encryption Scheme With Hidden Policy for Smart Medical Cloud. *IEEE Systems Journal*, **2021**, 15, 365-376	4.3	8
225	Multiauthority Access Control With Anonymous Authentication for Personal Health Record. *IEEE Internet of Things Journal*, **2021**, 8, 156-167	10.7	11
224	Privacy-Aware Image Authentication from Cryptographic Primitives. *Computer Journal*, **2021**, 64, 1178-1192	1.3	1
223	Scalable and redactable blockchain with update and anonymity. *Information Sciences*, **2021**, 546, 25-41	7.7	11
222	An Enhanced Certificateless Aggregate Signature Without Pairings for E-Healthcare System. *IEEE Internet of Things Journal*, **2021**, 8, 5000-5008	10.7	3
221	Secure and Efficient Data Aggregation for IoT Monitoring Systems. *IEEE Internet of Things Journal*, **2021**, 8, 8056-8063	10.7	4
220	Multicopy provable data possession scheme supporting data dynamics for cloud-based Electronic Medical Record system. *Information Sciences*, **2021**, 545, 254-276	7.7	9
219	. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 563-575	3.9	4
218	Unlinkable and Revocable Secret Handshake. *Computer Journal*, **2021**, 64, 1303-1314	1.3	0
217	Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT. *IEEE Transactions on Cloud Computing*, **2021**, 1-1	3.3	0

216	Privacy-Preserving Reverse Nearest Neighbor Query over Encrypted Spatial Data. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	2
215	Secure and Privacy-Preserved Data Collection for IoT Wireless Sensors. *IEEE Internet of Things Journal*, **2021**, 1-1	10.7	1
214	Distributed Ciphertext-Policy Attribute-Based Encryption With Enhanced Collusion Resilience and Privacy Preservation. *IEEE Systems Journal*, **2021**, 1-12	4.3	2
213	Secure Outsourced Attribute-based Sharing Framework for Lightweight Devices in Smart Health Systems. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	5
212	Privacy-Preserving Flexible Access Control for Encrypted Data in Internet of Things. *IEEE Internet of Things Journal*, **2021**, 8, 14731-14745	10.7	2
211	Bidirectional and Malleable Proof-of-Ownership for Large File in Cloud Storage. *IEEE Transactions on Cloud Computing*, **2021**, 1-1	3.3	1
210	Efficient and secure image authentication with robustness and versatility. *Science China Information Sciences*, **2020**, 63, 1	3.4	2
209	A code-based signature scheme from the Lyubashevsky framework. *Theoretical Computer Science*, **2020**, 835, 15-30	1.1	3
208	Authenticated Data Redaction with Accountability and Transparency. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	3
207	Outsourcing Attributed-Based Ranked Searchable Encryption With Revocation for Cloud Storage. *IEEE Access*, **2020**, 8, 104344-104356	3.5	6
206	Secure and Privacy-Preserving Attribute-Based Sharing Framework in Vehicles Ad Hoc Networks. *IEEE Access*, **2020**, 8, 116781-116795	3.5	1
205	Privacy-Preserving Multi-Authority Attribute-Based Data Sharing Framework for Smart Grid. *IEEE Access*, **2020**, 8, 23294-23307	3.5	10
204	An improved Durandal signature scheme. *Science China Information Sciences*, **2020**, 63, 1	3.4	1
203	HUCDO. *ACM Transactions on Cyber-Physical Systems*, **2020**, 4, 1-23	2.3	1
202	EVA: Efficient Versatile Auditing Scheme for IoT-Based Datamarket in Jointcloud. *IEEE Internet of Things Journal*, **2020**, 7, 882-892	10.7	11
201	Achieving Intelligent Trust-Layer for Internet-of-Things via Self-Redactable Blockchain. *IEEE Transactions on Industrial Informatics*, **2020**, 16, 2677-2686	11.9	18
200	Novel updatable identity-based hash proof system and its applications. *Theoretical Computer Science*, **2020**, 804, 1-28	1.1	1
199	Black-Box Accountable Authority Identity-Based Revocation System. *Computer Journal*, **2020**, 63, 525-535	1.3	0

198	A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. *Information Sciences*, **2020**, 516, 331-345	7.7	3
197	Identity-based encryption with leakage-amplified chosen-ciphertext attacks security. *Theoretical Computer Science*, **2020**, 809, 277-295	1.1	3
196	On the Security of Symmetric Encryption Against Mass Surveillance. *IEEE Access*, **2020**, 8, 175625-175636	3.5	
195	Secure Data Sharing With Lightweight Computation in E-Health. *IEEE Access*, **2020**, 8, 209630-209643	3.5	1
194	Multi-User Verifiable Searchable Symmetric Encryption for Cloud Storage. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 17, 1322-1332	3.9	27
193	Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing. *IEEE Systems Journal*, **2020**, 14, 387-397	4.3	12
192	Privacy-enhanced remote data integrity checking with updatable timestamp. *Information Sciences*, **2020**, 527, 210-226	7.7	4
191	Cloud-based Outsourcing for Enabling Privacy-Preserving Large-scale Non-Negative Matrix Factorization. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	16
190	Top-Level Secure Certificateless Signature Against Malicious-But-Passive KGC. *IEEE Access*, **2019**, 7, 112870-112878	3.5	28
189	ACE with Compact Ciphertext Size and Decentralized Sanitizers. *International Journal of Foundations of Computer Science*, **2019**, 30, 531-549	0.6	3
188	Continuous leakage-resilient identity-based encryption with leakage amplification. *Designs, Codes, and Cryptography*, **2019**, 87, 2061-2090	1.2	4
187	Strongly leakage resilient authenticated key exchange, revisited. *Designs, Codes, and Cryptography*, **2019**, 87, 2885-2911	1.2	5
186	Publicly verifiable secure communication with user and data privacy. *Personal and Ubiquitous Computing*, **2019**, 1	2.1	
185	A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Generation Computer Systems*, **2019**, 97, 284-294	7.5	37
184	Hidden Ciphertext Policy Attribute-Based Encryption With Fast Decryption for Personal Health Record System. *IEEE Access*, **2019**, 7, 33202-33213	3.5	28
183	Privacy-Preserving Certificateless Cloud Auditing with Multiple Users. *Wireless Personal Communications*, **2019**, 106, 1161-1182	1.9	11
182	. *IEEE Transactions on Industrial Informatics*, **2019**, 15, 3670-3679	11.9	37
181	On the Security of an Efficient and Robust Certificateless Signature Scheme for IIoT Environments. *IEEE Access*, **2019**, 7, 91074-91079	3.5	15

180	Provably Secure (Broadcast) Homomorphic Signcryption. *International Journal of Foundations of Computer Science*, **2019**, 30, 511-529	0.6	6
179	Fully Secure Lightweight Certificateless Signature Scheme for IIoT. *IEEE Access*, **2019**, 7, 144433-144443	3.5	15
178	Policy-Driven Blockchain and Its Applications for Transport Systems. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	9
177	Efficient Micropayment of Cryptocurrency from Blockchains. *Computer Journal*, **2019**, 62, 507-517	1.3	7
176	Anonymous and Updatable Identity-Based Hash Proof System. *IEEE Systems Journal*, **2019**, 13, 2818-2829	4.3	4
175	Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Information Sciences*, **2019**, 479, 116-134	7.7	45
174	Efficient identity-based broadcast encryption with keyword search against insider attacks for database systems. *Theoretical Computer Science*, **2019**, 767, 51-72	1.1	6
173	Threshold privacy-preserving cloud auditing with multiple uploaders. *International Journal of Information Security*, **2019**, 18, 321-331	2.8	3
172	The generic construction of continuous leakage-resilient identity-based cryptosystems. *Theoretical Computer Science*, **2019**, 772, 1-45	1.1	7
171	. *IEEE Transactions on Information Forensics and Security*, **2018**, 13, 2101-2113	8	55
170	New Approach for Privacy-Aware Location-Based Service Communications. *Wireless Personal Communications*, **2018**, 101, 1057-1073	1.9	6
169	Witness-based searchable encryption. *Information Sciences*, **2018**, 453, 364-378	7.7	10
168	Security of Grouping-Proof Authentication Protocol for Distributed RFID Systems. *IEEE Wireless Communications Letters*, **2018**, 7, 254-257	5.9	8
167	Efficient k -out-of- n oblivious transfer scheme with the ideal communication cost. *Theoretical Computer Science*, **2018**, 714, 15-26	1.1	4
166	Practical and secure telemedicine systems for user mobility. *Journal of Biomedical Informatics*, **2018** , 78, 24-32	10.2	19
165	Privacy-enhanced attribute-based private information retrieval. *Information Sciences*, **2018**, 454-455, 275-291	7.7	7
164	Continuous Leakage-Resilient Identity-Based Encryption without Random Oracles. *Computer Journal*, **2018**, 61, 586-600	1.3	17
163	Improving Privacy-Preserving and Security for Decentralized Key-Policy Attributed-Based Encryption. *IEEE Access*, **2018**, 6, 12736-12745	3.5	13

162	A New Revocable and Re-Delegable Proxy Signature and Its Application. *Journal of Computer Science and Technology*, **2018**, 33, 380-399	1.7	2
161	Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*, **2018**, 78, 720-729	7.5	64
160	Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. *International Journal of Information Security*, **2018**, 17, 463-475	2.8	11
159	A Privacy-Preserving Fog Computing Framework for Vehicular Crowdsensing Networks. *IEEE Access*, **2018**, 6, 43776-43784	3.5	34
158	Policy controlled system with anonymity. *Theoretical Computer Science*, **2018**, 745, 87-113	1.1	2
157	A Generic Scheme of plaintext-checkable database encryption. *Information Sciences*, **2018**, 429, 88-101	7.7	12
156	Improving Privacy-Preserving CP-ABE with Hidden Access Policy. *Lecture Notes in Computer Science*, **2018**, 596-605	0.9	5
155	A Novel Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Anonymous Key Generation. *Lecture Notes in Computer Science*, **2018**, 435-446	0.9	2
154	Efficient Traceable Oblivious Transfer and Its Applications. *Lecture Notes in Computer Science*, **2018**, 610-621	0.9	1
153	Strong Identity-Based Proxy Signature Schemes, Revisited. *Wireless Communications and Mobile Computing*, **2018**, 2018, 1-11	1.9	3
152	Introduction to Security Reduction **2018**,		7
151	A new generic construction of anonymous designated confirmer signature for privacy-preserving fair exchange. *International Journal of Computer Mathematics*, **2017**, 94, 946-961	1.2	
150	Efficient identity-based online/offline encryption and signcryption with short ciphertext. *International Journal of Information Security*, **2017**, 16, 299-311	2.8	16
149	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. *IEEE Systems Journal*, **2017**, 11, 1018-1026	4.3	12
148	Privacy-preserving data search and sharing protocol for social networks through wireless applications. *Concurrency Computation Practice and Experience*, **2017**, 29, e3870	1.4	3
147	A Generic Table Recomputation-Based Higher-Order Masking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **2017**, 36, 1779-1789	2.5	1
146	Private Keyword-Search for Database Systems Against Insider Attacks. *Journal of Computer Science and Technology*, **2017**, 32, 599-617	1.7	16
145	Privacy-Preserving Data Packet Filtering Protocol with Source IP Authentication. *Wireless Personal Communications*, **2017**, 95, 3509-3537	1.9	

144	Strong authenticated key exchange with auxiliary inputs. *Designs, Codes, and Cryptography*, **2017**, 85, 145-173	1.2	26
143	Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. *Quantum Information Processing*, **2017**, 16, 1	1.6	4
142	Secure-channel free keyword search with authorization in manager-centric databases. *Computers and Security*, **2017**, 69, 50-64	4.9	6
141	Provably Secure Homomorphic Signcryption. *Lecture Notes in Computer Science*, **2017**, 349-360	0.9	11
140	Designated Verifier Proxy Re-signature for Deniable and Anonymous Wireless Communications. *Wireless Personal Communications*, **2017**, 97, 3017-3030	1.9	8
139	Fuzzy Extractors for Biometric Identification **2017**,		6
138	Privacy-Preserving Mutual Authentication in RFID with Designated Readers. *Wireless Personal Communications*, **2017**, 96, 4819-4845	1.9	4
137	Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city. *Personal and Ubiquitous Computing*, **2017**, 21, 855-868	2.1	13
136	Policy-controlled signatures and their applications. *Computer Standards and Interfaces*, **2017**, 50, 26-41	3.5	4
135	Identity-based provable data possession revisited: Security analysis and generic construction. *Computer Standards and Interfaces*, **2017**, 54, 10-19	3.5	16
134	Efficient E-coupon systems with strong user privacy. *Telecommunication Systems*, **2017**, 64, 695-708	2.3	6
133	Privacy-Preserving Yoking Proof with Key Exchange in the Three-Party Setting. *Wireless Personal Communications*, **2017**, 94, 1017-1034	1.9	5
132	Efficient dynamic threshold identity-based encryption with constant-size ciphertext. *Theoretical Computer Science*, **2016**, 609, 49-59	1.1	2
131	Trust-based group services selection in web-based service-oriented environments. *World Wide Web*, **2016**, 19, 807-832	2.9	3
130	Generalized closest substring encryption. *Designs, Codes, and Cryptography*, **2016**, 80, 103-124	1.2	
129	Multi-authority security framework for scalable EHR systems. *International Journal of Medical Engineering and Informatics*, **2016**, 8, 390	0.5	2
128	Server-Aided Public Key Encryption With Keyword Search. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 2833-2842	8	101
127	An efficient privacy-preserving aggregation and billing protocol for smart grid. *Security and Communication Networks*, **2016**, 9, 4536-4547	1.9	20

126	Secure Multiparty Quantum Computation for Summation and Multiplication. *Scientific Reports*, **2016**, 6, 19655	4.9	48
125	CCA2 secure public-key encryption scheme tolerating continual leakage attacks. *Security and Communication Networks*, **2016**, 9, 4505-4519	1.9	15
124	Privacy-Preserving and Secure Sharing of PHR in the Cloud. *Journal of Medical Systems*, **2016**, 40, 267	5.1	17
123	An efficient quantum scheme for Private Set Intersection. *Quantum Information Processing*, **2016**, 15, 363-371	1.6	22
122	Recipient Revocable Identity-Based Broadcast Encryption **2016**,		17
121	Comments on Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 658-659	8	24
120	Comments on Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks *IEEE Transactions on Wireless Communications*, **2016**, 15, 3097-3099	9.6	4
119	Strongly Leakage-Resilient Authenticated Key Exchange. *Lecture Notes in Computer Science*, **2016**, 19-36	0.9	19
118	Distributed clinical data sharing via dynamic access-control policy transformation. *International Journal of Medical Informatics*, **2016**, 89, 25-31	5.3	24
117	Online/Offline Ciphertext Retrieval on Resource Constrained Devices. *Computer Journal*, **2016**, 59, 955-969	1.3	13
116	Privacy-Preserving Cloud Auditing with Multiple Uploaders. *Lecture Notes in Computer Science*, **2016** , 224-237	0.9	9
115	Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. *Lecture Notes in Computer Science*, **2016**, 223-239	0.9	20
114	Proxy Signature with Revocation. *Lecture Notes in Computer Science*, **2016**, 21-36	0.9	2
113	Comment on Secure quantum private information retrieval using phase-encoded queries *Physical Review A*, **2016**, 94,	2.6	11
112	Relations between robustness and RKA security under public-key encryption. *Theoretical Computer Science*, **2016**, 628, 78-91	1.1	2
111	Compact Anonymous Hierarchical Identity-Based Encryption with Constant Size Private Keys. *Computer Journal*, **2016**, 59, 452-461	1.3	5
110	One-Round Privacy-Preserving Meeting Location Determination for Smartphone Applications. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1712-1721	8	11
109	Secure Channel Free ID-Based Searchable Encryption for Peer-to-Peer Group. *Journal of Computer Science and Technology*, **2016**, 31, 1012-1027	1.7	22

108	Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 665-678	8	87
107	Proof of retrievability with public verifiability resilient against related-key attacks. *IET Information Security*, **2015**, 9, 43-49	1.4	13
106	Identity-based quotable ring signature. *Information Sciences*, **2015**, 321, 71-89	7.7	6
105	Loss-Tolerant Bundle Fragment Authentication for Space-Based DTNs. *IEEE Transactions on Dependable and Secure Computing*, **2015**, 12, 615-625	3.9	2
104	BL-MLE: Block-Level Message-Locked Encryption for Secure Large File Deduplication. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 2643-2652	8	62
103	A New Public Remote Integrity Checking Scheme with User Privacy. *Lecture Notes in Computer Science*, **2015**, 377-394	0.9	8
102	AAC-OT: Accountable Oblivious Transfer With Access Control. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 2502-2514	8	10
101	Provably Secure Identity Based Provable Data Possession. *Lecture Notes in Computer Science*, **2015**, 310-325	0.9	14
100	Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security*, **2015**, 14, 307-318	2.8	53
99	Key management for Smart Grid based on asymmetric key-wrapping. *International Journal of Computer Mathematics*, **2015**, 92, 498-512	1.2	3
98	Comments on a Public Auditing Mechanism for Shared Cloud Data Service. *IEEE Transactions on Services Computing*, **2015**, 8, 998-999	4.8	32
97	An IPv6-based mobility framework for urban vehicular networks. *International Journal of Network Management*, **2015**, 25, 141-158	1.8	0
96	Quantum oblivious set-member decision protocol. *Physical Review A*, **2015**, 92,	2.6	25
95	Two Quantum Protocols for Oblivious Set-member Decision Problem. *Scientific Reports*, **2015**, 5, 15914	4.9	8
94	Vulnerabilities of an ECC-based RFID authentication scheme. *Security and Communication Networks*, **2015**, 8, 3262-3270	1.9	4
93	Fully Secure Hierarchical Inner Product Encryption for Privacy Preserving Keyword Searching in Cloud **2015**,		1
92	Further ideal multipartite access structures from integer polymatroids. *Science China Information Sciences*, **2015**, 58, 1-13	3.4	
91	A resilient identity-based authenticated key exchange protocol. *Security and Communication Networks*, **2015**, 8, 2279-2290	1.9	7

90	Improved Identity-Based Online/Offline Encryption. *Lecture Notes in Computer Science*, **2015**, 160-173	0.9	9
89	A New General Framework for Secure Public Key Encryption with Keyword Search. *Lecture Notes in Computer Science*, **2015**, 59-76	0.9	33
88	Identity based identification from algebraic coding theory. *Theoretical Computer Science*, **2014**, 520, 51-61	1.1	6
87	A Secure IPv6 Address Configuration Protocol for Vehicular Networks. *Wireless Personal Communications*, **2014**, 79, 721-744	1.9	11
86	Subset Membership Encryption and Its Applications to Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 1098-1107	8	16
85	On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. *IEEE Transactions on Parallel and Distributed Systems*, **2014**, 25, 2760-2761	3.7	41
84	Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 5-13	8	15
83	Security pitfalls of an efficient threshold proxy signature scheme for mobile agents. *Information Processing Letters*, **2014**, 114, 5-8	0.8	2
82	CP-ABE With Constant-Size Keys for Lightweight Devices. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 763-771	8	98
81	Towards a cryptographic treatment of publish/subscribe systems1. *Journal of Computer Security*, **2014**, 22, 33-67	0.8	6
80	Anonymous Proxy Signature with Restricted Traceability **2014**,		3
79	Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage. *Lecture Notes in Computer Science*, **2014**, 28-40	0.9	19
78	Trust-oriented QoS-aware composite service selection based on genetic algorithms. *Concurrency Computation Practice and Experience*, **2014**, 26, 500-515	1.4	16
77	Efficient public key encryption with revocable keyword search. *Security and Communication Networks*, **2014**, 7, 466-472	1.9	23
76	A secure mobility support scheme for 6LoWPAN wireless sensor networks. *Security and Communication Networks*, **2014**, 7, 641-652	1.9	5
75	Public-Key Encryption Resilient against Linear Related-Key Attacks Revisited **2014**,		2
74	Privacy-Preserving Authorized RFID Authentication Protocols. *Lecture Notes in Computer Science*, **2014**, 108-122	0.9	6
73	Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding. *Journal of Lightwave Technology*, **2013**, 31, 2533-2539	4	68

72	A robust trust model for service-oriented systems. *Journal of Computer and System Sciences*, **2013**, 79, 596-608	1	15
71	On security of a certificateless signcryption scheme. *Information Sciences*, **2013**, 232, 475-481	7.7	20
70	Identity-based data storage in cloud computing. *Future Generation Computer Systems*, **2013**, 29, 673-681	7.5	50
69	Membership Encryption and Its Applications. *Lecture Notes in Computer Science*, **2013**, 219-234	0.9	9
68	Leakage Resilient Authenticated Key Exchange Secure in the Auxiliary Input Model. *Lecture Notes in Computer Science*, **2013**, 204-217	0.9	13
67	Constant-Size Dynamic K-Times Anonymous Authentication. *IEEE Systems Journal*, **2013**, 7, 249-261	4.3	17
66	Identity-Based Mediated RSA Revisited **2013**,		1
65	Anonymous Identity-Based Broadcast Encryption with Adaptive Security. *Lecture Notes in Computer Science*, **2013**, 258-271	0.9	14
64	Privacy enhanced data outsourcing in the cloud. *Journal of Network and Computer Applications*, **2012**, 35, 1367-1373	7.9	27
63	New constructions of OSBE schemes and their applications in oblivious access control. *International Journal of Information Security*, **2012**, 11, 389-401	2.8	1
62	Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, **2012**, 23, 2150-2162	3.7	95
61	Privacy preserving protocol for service aggregation in cloud computing. *Software - Practice and Experience*, **2012**, 42, 467-483	2.5	
60	Efficient oblivious transfers with access control. *Computers and Mathematics With Applications*, **2012**, 63, 827-837	2.7	5
59	Efficient and secure stored-value cards with leakage resilience. *Computers and Electrical Engineering* , **2012**, 38, 370-380	4.3	
58	Certificateless Signatures: New Schemes and Security Models. *Computer Journal*, **2012**, 55, 457-474	1.3	63
57	Provably Secure Single Sign-on Scheme in Distributed Systems and Networks **2012**,		7
56	Further Analysis of a Practical Hierarchical Identity-Based Encryption Scheme. *IEICE Transactions on Information and Systems*, **2012**, E95.D, 1690-1693	0.6	
55	Privacy-Preserved Access Control for Cloud Computing **2011**,		13

54	Case-Based Trust Evaluation from Provenance Information **2011**,		6
53	Optimistic Fair Exchange with Strong Resolution-Ambiguity. *IEEE Journal on Selected Areas in Communications*, **2011**, 29, 1491-1502	14.2	4
52	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 498-512	8	20
51	Secure mobile agents with controlled resources. *Concurrency Computation Practice and Experience*, **2011**, 23, 1348-1366	1.4	1
50	Web Service Selection Based on Similarity Evaluation **2011**,		3
49	Provably secure server-aided verification signatures. *Computers and Mathematics With Applications*, **2011**, 61, 1705-1723	2.7	18
48	Strongly unforgeable proxy signature scheme secure in the standard model. *Journal of Systems and Software*, **2011**, 84, 1471-1479	3.3	18
47	Short Signatures with a Tighter Security Reduction Without Random Oracles. *Computer Journal*, **2011**, 54, 513-524	1.3	2
46	Practical RFID ownership transfer scheme. *Journal of Computer Security*, **2011**, 19, 319-341	0.8	13
45	GTrust: An Innovated Trust Model for Group Services Selection in Web-Based Service-Oriented Environments. *Lecture Notes in Computer Science*, **2011**, 306-313	0.9	4
44	Efficient RFID Authentication Scheme for Supply Chain Applications **2010**,		3
43	Dynamic Trust Model for Federated Identity Management **2010**,		9
42	Constructions of certificate-based signature secure against key replacement attacks*. *Journal of Computer Security*, **2010**, 18, 421-449	0.8	28
41	PBTrust: A Priority-Based Trust Model for Service Selection in General Service-Oriented Environments **2010**,		4
40	How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, **2010**, 9, 297-311	2.8	20
39	Certificateless threshold signature scheme from bilinear maps. *Information Sciences*, **2010**, 180, 4714-4728	7.7	22
38	Certificateless Threshold Ring Signature. *Information Sciences*, **2009**, 179, 3685-3696	7.7	38
37	An Efficient Certificateless Encryption Scheme in the Standard Model **2009**,		4

36	Secure Mobile Agents with Designated Hosts **2009**,		2
35	Universal Designated Verifier Signatures with Threshold-Signers. *Lecture Notes in Computer Science*, **2009**, 89-109	0.9	3
34	Identity-Based Online/Offline Encryption. *Lecture Notes in Computer Science*, **2008**, 247-261	0.9	39
33	Optimal Online/Offline Signature: How to Sign a Message without Online Computation. *Lecture Notes in Computer Science*, **2008**, 98-111	0.9	7
32	Identity-Based On-Line/Off-Line Signcryption **2008**,		14
31	Cryptanalysis and improvement of an efficient certificateless signature scheme. *Journal of Communications and Networks*, **2008**, 10, 10-17	4.1	12
30	A Generic Construction of Identity-Based Online/Offline Signcryption **2008**,		9
29	Hierarchical Identity-Based Online/Offline Encryption **2008**,		4
28	Multi-identity management for identity-based cryptography. *Journal of Discrete Mathematical Sciences and Cryptography*, **2008**, 11, 639-672	1.7	3
27	Securing wireless mesh networks with ticket-based authentication **2008**,		10
26	Cryptanalysis of simple three-party key exchange protocol. *Computers and Security*, **2008**, 27, 16-21	4.9	54
25	Secure universal designated verifier signature without random oracles. *International Journal of Information Security*, **2008**, 7, 171-183	2.8	24
24	Practical Anonymous Divisible E-Cash from Bounded Accumulators. *Lecture Notes in Computer Science*, **2008**, 287-301	0.9	24
23	Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacrypt□004. *Journal of Computer Science and Technology*, **2007**, 22, 71-74	1.7	
22	Revocable Ring Signature. *Journal of Computer Science and Technology*, **2007**, 22, 785-794	1.7	37
21	Short Group Signatures Without Random Oracles. *Journal of Computer Science and Technology*, **2007**, 22, 805-821	1.7	
20	Certificateless Signature Revisited **2007**, 308-322		115
19	Certificate-Based Signature: Security Model and Efficient Construction. *Lecture Notes in Computer Science*, **2007**, 110-125	0.9	32

18	Server-Aided Public Key Generation Protocols on Low-power Devices for Ad-hoc Networks **2006**,		2
17	Proxy Signature Without Random Oracles. *Lecture Notes in Computer Science*, **2006**, 473-484	0.9	22
16	Certificateless Designated Verifier Signature Schemes **2006**,		3
15	Ad Hoc Group Signatures. *Lecture Notes in Computer Science*, **2006**, 120-135	0.9	7
14	Short (Identity-Based) Strong Designated Verifier Signature Schemes. *Lecture Notes in Computer Science*, **2006**, 214-225	0.9	15
13	Three-Round Secret Handshakes Based on ElGamal and DSA. *Lecture Notes in Computer Science*, **2006**, 332-342	0.9	13
12	Constant-Size Dynamic k-TAA. *Lecture Notes in Computer Science*, **2006**, 111-125	0.9	110
11	Universal Designated Verifier Signature Without Delegatability. *Lecture Notes in Computer Science*, **2006**, 479-498	0.9	17
10	A New Signature Scheme Without Random Oracles from Bilinear Pairings. *Lecture Notes in Computer Science*, **2006**, 67-80	0.9	14
9	A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World. *Lecture Notes in Computer Science*, **2005**, 480-489	0.9	18
8	Identity-Based Universal Designated Verifier Signatures. *Lecture Notes in Computer Science*, **2005**, 825-834	0.9	14
7	On the Security of Certificateless Signature Schemes from Asiacrypt 2003. *Lecture Notes in Computer Science*, **2005**, 13-25	0.9	113
6	Identity-Based Strong Designated Verifier Signature Schemes. *Lecture Notes in Computer Science*, **2004**, 313-324	0.9	45
5	Robust non-interactive oblivious transfer. *IEEE Communications Letters*, **2003**, 7, 153-155	3.8	10
4	m out of n Oblivious Transfer. *Lecture Notes in Computer Science*, **2002**, 395-405	0.9	21
3	A Fair Electronic Cash Scheme. *Lecture Notes in Computer Science*, **2001**, 20-32	0.9	9
2	Privacy-enhanced Internet storage		2
1	Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world		12