Kaitai Liang

List of Publications by Year
in descending order

88	2,948	186265	182427
papers	citations	28	51
		h-index	g-index

90	90	90	2234
all docs	docs citations	times ranked	citing authors

#	ARTICLE	IF	CITATIONS
1	Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1981-1992.	6.9	172
2	Auditable σ -Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2018, 13, 94-105.	6.9	157
3	Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2018, 14, 3618-3627.	11.3	155
4	BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular <i>Ad Hoc</i> Networks. IEEE Transactions on Industrial Informatics, 2020, 16, 4146-4155.	11.3	150
5	An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Generation Computer Systems, 2018, 78, 753-762.	7.5	132
6	A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Future Generation Computer Systems, 2015, 52, 95-108.	7.5	128
7	A blockchain-based location privacy-preserving crowdsensing system. Future Generation Computer Systems, 2019, 94, 408-418.	7.5	128
8	Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2016, 11, 1661-1673.	6.9	122
9	Cost-Effective Authentic and Anonymous Data Sharing with Forward Security. IEEE Transactions on Computers, 2015, 64, 971-983.	3.4	93
10	An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing. Lecture Notes in Computer Science, 2014, , 257-272.	1.3	92
11	A Ciphertext-Policy Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security. , 2013, , .		85
12	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.	6.9	85
13	Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1578-1589.	6.9	81
14	Passive Attacks Against Searchable Encryption. IEEE Transactions on Information Forensics and Security, 2019, 14, 789-802.	6.9	77
15	Searchain: Blockchain-based private keyword search in decentralized storage. Future Generation Computer Systems, 2020, 107, 781-792.	7.5	69
16	Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices. IEEE Systems Journal, 2019, 13, 2775-2785.	4.6	59
17	Secure sharing and searching for real-time video data in mobile cloud. IEEE Network, 2015, 29, 46-50.	6.9	57
18	Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 2016, 65, 1992-2004.	3.4	56

#	Article	IF	Citations
19	Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. Lecture Notes in Computer Science, 2015, , 146-166.	1.3	54
20	Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List. Lecture Notes in Computer Science, 2018, , 516-534.	1.3	54
21	Am I eclipsed? A smart detector of eclipse attacks for Ethereum. Computers and Security, 2020, 88, 101604.	6.0	50
22	Lightweight Searchable Encryption Protocol for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2021, 17, 4248-4259.	11.3	49
23	Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theoretical Computer Science, 2014, 539, 87-105.	0.9	47
24	Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data. IEEE Transactions on Information Forensics and Security, 2016, 11, 2365-2376.	6.9	47
25	Toward Practical Privacy-Preserving Processing Over Encrypted Data in IoT: An Assistive Healthcare Use Case. IEEE Internet of Things Journal, 2019, 6, 10177-10190.	8.7	41
26	Privacy Concerns for Photo Sharing in Online Social Networks. IEEE Internet Computing, 2015, 19, 58-63.	3.3	33
27	CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage. IEEE Transactions on Services Computing, 2019, , 1-1.	4.6	33
28	Privacy-preserving personal data operation on mobile cloudâ€”Chances and challenges over advanced persistent threat. Future Generation Computer Systems, 2018, 79, 337-349.	7.5	32
29	Trust2Privacy: A Novel Fuzzy Trust-to-Privacy Mechanism for Mobile Social Networks. IEEE Wireless Communications, 2020, 27, 72-78.	9.0	29
30	An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing. Lecture Notes in Computer Science, 2014, , 448-461.	1.3	28
31	A Cloud-Based Access Control Scheme withÂUser Revocation and Attribute Update. Lecture Notes in Computer Science, 2016, , 525-540.	1.3	26
32	Secure bidirectional proxy re-encryption for cryptographic cloud storage. Pervasive and Mobile Computing, 2016, 28, 113-121.	3.3	26
33	A Security-Enhanced Certificateless Aggregate Signature Authentication Protocol for InVANETs. IEEE Network, 2020, 34, 22-29.	6.9	25
34	A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles. Lecture Notes in Computer Science, 2013, , 231-246.	1.3	24
35	Dual Access Control for Cloud-Based Data Storage and Sharing. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	23
36	Distributed additive encryption and quantization for privacy preserving federated deep learning. Neurocomputing, 2021, 463, 309-327.	5.9	23

#	Article	IF	Citations
37	A ciphertext‐policy attribute‐based proxy re‐encryption scheme for data sharing in public clouds. Concurrency Computation Practice and Experience, 2015, 27, 2004-2027.	2.2	22
38	Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation. Computer Journal, 2017, 60, 1210-1222.	2.4	22
39	Polynomial-based modifiable blockchain structure for removing fraud transactions. Future Generation Computer Systems, 2019, 99, 154-163.	7.5	20
40	A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release. Lecture Notes in Computer Science, 2013, , 132-146.	1.3	20
41	Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. Computer Journal, 2015, 58, 2778-2792.	2.4	18
42	Expressive attribute-based keyword search with constant-size ciphertext. Soft Computing, 2018, 22, 5163-5177.	3.6	18
43	Efficient Multi-Function Data Sharing and Searching Mechanism for Cloud-Based Encrypted Data. , 2016, , .		17
44	SoProtector: Safeguard Privacy for Native SO Files in Evolving Mobile IoT Applications. IEEE Internet of Things Journal, 2020, 7, 2539-2552.	8.7	16
45	Efficient Encrypted Data Search With Expressive Queries and Flexible Update. IEEE Transactions on Services Computing, 2022, 15, 1619-1633.	4.6	16
46	ROSE: Robust Searchable Encryption With Forward and Backward Security. IEEE Transactions on Information Forensics and Security, 2022, 17, 1115-1130.	6.9	16
47	DT-CP: A Double-TTPs-Based Contract-Signing Protocol With Lower Computational Cost. IEEE Access, 2019, 7, 174740-174749.	4.2	14
48	Secure Edge Computing with Lightweight Control-Flow Property-based Attestation. , 2019, , .		13
49	Fine-grained information flow control using attributes. Information Sciences, 2019, 484, 167-182.	6.9	13
50	A Behavior Based Trustworthy Service Composition Discovery Approach in Cloud Environment. IEEE Access, 2019, 7, 56492-56503.	4.2	13
51	An efficient blind filter: Location privacy protection and the access control in FinTech. Future Generation Computer Systems, 2019, 100, 797-810.	7.5	12
52	An Efficient Attribute-Based Multi-Keyword Search Scheme in Encrypted Keyword Generation. IEEE Access, 2020, 8, 99024-99036.	4.2	11
53	Practical Threshold Multi-Factor Authentication. IEEE Transactions on Information Forensics and Security, 2021, 16, 3573-3588.	6.9	11
54	A data hiding approach for sensitive smartphone data. , 2016, , .		10

#	Article	IF	Citations
55	Using Sparse Representation to Detect Anomalies in Complex WSNs. ACM Transactions on Intelligent Systems and Technology, 2019, 10, 1-18.	4.5	9
56	Broadcast encryption with dealership. International Journal of Information Security, 2016, 15, 271-283.	3.4	8
57	Encryption Switching Service: Securely Switch Your Encrypted Data to Another Format. IEEE Transactions on Services Computing, 2021, 14, 1357-1369.	4.6	8
58	An Efficient Key-Policy Attribute-Based Searchable Encryption in Prime-Order Groups. Lecture Notes in Computer Science, 2017, , 39-56.	1.3	7
59	Efficient Attribute-Based Data Sharing Scheme with Hidden Access Structures. Computer Journal, 2019, 62, 1748-1760.	2.4	7
60	How to implement secure cloud file sharing using optimized attribute-based access control with small policy matrix and minimized cumulative errors. Computers and Security, 2021, 107, 102318.	6.0	7
61	Cost-effective privacy-preserving vehicular urban sensing system. Personal and Ubiquitous Computing, 2017, 21, 893-901.	2.8	6
62	TAW: Cost-Effective Threshold Authentication With Weights for Internet of Things. IEEE Access, 2019, 7, 30112-30125.	4.2	6
63	Message Integration Authentication in the Internet-of-Things via Lattice-Based Batch Signatures. Sensors, 2018, 18, 4056.	3.8	4
64	Secure and efficient access of personal health record: a group-oriented ciphertext-policy attribute-based encryption. Journal of the Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers,Series A/Chung-kuo Kung Ch'eng Hsuch K'an, 2019, 42, 80-86.	1.1	4
65	On-the-Fly Privacy for Location Histograms. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 566-578.	5.4	4
66	Post quantum proxy signature scheme based on the multivariate public key cryptographic signature. International Journal of Distributed Sensor Networks, 2020, 16, 155014772091477.	2.2	4
67	Improved Probabilistic Context-Free Grammars for Passwords Using Word Extraction. , 2021, , .		4
68	Online/Offline Public-Index Predicate Encryption for Fine-Grained Mobile Access Control. Lecture Notes in Computer Science, 2016, , 588-605.	1.3	3
69	Anonymous Proxy Signature with Hierarchical Traceability: TABLE 1.. Computer Journal, 2016, 59, 559-569.	2.4	3
70	DABEHR: Decentralized Attribute-Based Electronic Health Record System with Constant-Size Storage Complexity. Lecture Notes in Computer Science, 2017, , 611-626.	1.3	3
71	One-Round Attribute-Based Key Exchange in the Multi-Party Setting. International Journal of Foundations of Computer Science, 2017, 28, 725-742.	1.1	3
72	Quantum-Resistant Identity-Based Signature with Message Recovery and Proxy Delegation. Symmetry, 2019, 11, 272.	2.2	3

#	Article	IF	Citations
73	JSCSP: a Novel Policy-Based XSS Defense Mechanism for Browsers. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	3
74	Privacy preserving search services against online attack. Computers and Security, 2020, 95, 101836.	6.0	3
75	Cryptanalysis of Raindrop and FBC. Lecture Notes in Computer Science, 2019, , 536-551.	1.3	3
76	A new unpredictabilityâ€based radio frequency identification forward privacy model and a provably secure construction. Security and Communication Networks, 2015, 8, 2836-2849.	1.5	2
77	One-Round Attribute-Based Key Exchange in the Multi-party Setting. Lecture Notes in Computer Science, 2016, , 227-243.	1.3	2
78	Delegation of Decryption Rights With Revocability From Learning With Errors. IEEE Access, 2018, 6, 61163-61175.	4.2	2
79	A New Encrypted Data Switching Protocol: Bridging IBE and ABE Without Loss of Data Confidentiality. IEEE Access, 2019, 7, 50658-50668.	4.2	2
80	Practical Attribute-Based Conjunctive Keyword Search Scheme. Computer Journal, 2020, 63, 1203-1215.	2.4	2
81	Deep Binarized Convolutional Neural Network Inferences over Encrypted Data. , 2020, , .		2
82	A New Transitive Signature Scheme. Lecture Notes in Computer Science, 2016, , 156-167.	1.3	2
83	Secret Picture: An Efficient Tool for Mitigating Deletion Delay on OSN. Lecture Notes in Computer Science, 2016, , 467-477.	1.3	1
84	Hierarchical Conditional Proxy Re-Encryption: A New Insight of Fine-Grained Secure Data Sharing. Lecture Notes in Computer Science, 2017, , 118-135.	1.3	1
85	CCA Secure Public Key Encryption against After-the-Fact Leakage without NIZK Proofs. Security and Communication Networks, 2019, 2019, 1-8.	1.5	1
86	Defending Use-After-Free via Relationship Between Memory and Pointer. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 583-597.	0.3	1
87	Secure and Traceable Framework for Data Circulation. Lecture Notes in Computer Science, 2016, , 376-388.	1.3	0
88	A Modified Segmentation Approach for Overlapping Elliptical Objects with Various Sizes. Lecture Notes in Computer Science, 2017, , 222-236.	1.3	0