Joseph K Liu

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/792754/publications.pdf

Version: 2024-02-01

135 papers	5,595 citations	70961 41 h-index	102304 66 g-index
141 all docs	141 docs citations	141 times ranked	3357 citing authors

#	Article	IF	Citations
1	Achieving Searchable Encryption Scheme With Search Pattern Hidden. IEEE Transactions on Services Computing, 2022, 15, 1012-1025.	3.2	28
2	Forward and Backward Private DSSE for Range Queries. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 328-338.	3.7	20
3	A New Privacy-Preserving Payment Protocol for Blockchain Transactions. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 647-662.	3.7	5
4	Geometric Range Search on Encrypted Data With Forward/Backward Security. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 698-716.	3.7	7
5	Efficient Encrypted Data Search With Expressive Queries and Flexible Update. IEEE Transactions on Services Computing, 2022, 15, 1619-1633.	3.2	16
6	Non-Interactive Multi-Client Searchable Encryption: Realization and Implementation. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 452-467.	3.7	22
7	Practical Encrypted Network Traffic Pattern Matching for Secure Middleboxes. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2609-2621.	3.7	11
8	Privacy-Preserving and Outsourced Multi-Party K-Means Clustering Based on Multi-Key Fully Homomorphic Encryption. IEEE Transactions on Dependable and Secure Computing, 2022, , 1-12.	3.7	6
9	Efficient and Adaptive Procurement Protocol with Purchasing Privacy. IEEE Transactions on Services Computing, 2021, 14, 683-694.	3.2	0
10	Enabling Authorized Encrypted Search for Multi-Authority Medical Databases. IEEE Transactions on Emerging Topics in Computing, 2021, 9, 534-546.	3.2	15
11	hPRESS: A Hardware-Enhanced Proxy Re-Encryption Scheme Using Secure Enclave. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 1144-1157.	1.9	3
12	Geo-DRS: Geometric Dynamic Range Search on Spatial Data with Backward and Content Privacy. Lecture Notes in Computer Science, 2021, , 24-43.	1.0	3
13	Building a dynamic searchable encrypted medical database for multi-client. Information Sciences, 2020, 527, 394-405.	4.0	26
14	Attribute-Based Hybrid Boolean Keyword Search over Outsourced Encrypted Data. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 1207-1217.	3.7	45
15	DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT. IEEE Transactions on Industrial Informatics, 2020, 16, 2081-2090.	7.2	77
16	Practical Escrow Protocol for Bitcoin. IEEE Transactions on Information Forensics and Security, 2020, 15, 3023-3034.	4.5	9
17	Revocable and Linkable Ring Signature. Lecture Notes in Computer Science, 2020, , 3-27.	1.0	5
18	Multi-client Cloud-based Symmetric Searchable Encryption. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	17

#	Article	IF	Citations
19	GraphSEÂ². , 2019, , .		14
20	On The Unforkability of Monero. , 2019, , .		13
21	MatRiCT. , 2019, , .		61
22	Ring Signature. , 2019, , 93-114.		3
23	Dynamic Searchable Symmetric Encryption with Forward and Stronger Backward Privacy. Lecture Notes in Computer Science, 2019, , 283-303.	1.0	40
24	A Multi-client Dynamic Searchable Symmetric Encryption System with Physical Deletion. Lecture Notes in Computer Science, 2018, , 516-528.	1.0	1
25	Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices. IEEE Transactions on Industrial Informatics, 2018, 14, 3724-3732.	7.2	45
26	An efficient access control scheme with outsourcing capability and attribute update for fog computing. Future Generation Computer Systems, 2018, 78, 753-762.	4.9	132
27	Privacy-preserving personal data operation on mobile cloudâ€"Chances and challenges over advanced persistent threat. Future Generation Computer Systems, 2018, 79, 337-349.	4.9	32
28	Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage. IEEE Transactions on Information Forensics and Security, 2018, 13, 186-196.	4.5	49
29	Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control. Future Generation Computer Systems, 2018, 87, 712-724.	4.9	26
30	Result Pattern Hiding Searchable Encryption for Conjunctive Queries. , 2018, , .		113
31	Practical Backward-Secure Searchable Encryption from Symmetric Puncturable Encryption. , 2018, , .		125
32	GO-CP-ABE: group-oriented ciphertext-policy attribute-based encryption. International Journal of Embedded Systems, 2018, 10, 62.	0.2	3
33	Compact Ring Signature in the Standard Model for Blockchain. Lecture Notes in Computer Science, 2018, , 50-65.	1.0	4
34	Platform-Independent Secure Blockchain-Based Voting System. Lecture Notes in Computer Science, 2018, , 369-386.	1.0	75
35	Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). Lecture Notes in Computer Science, 2018, , 558-576.	1.0	50
36	Revocable Identity-Based Encryption from the Computational Diffie-Hellman Problem. Lecture Notes in Computer Science, 2018, , 265-283.	1.0	3

#	Article	IF	Citations
37	Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List. Lecture Notes in Computer Science, 2018, , 516-534.	1.0	54
38	Dynamic Searchable Symmetric Encryption Schemes Supporting Range Queries with Forward (and) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50	1.0	43
39	Towards Efficient Verifiable Conjunctive Keyword Search for Large Encrypted Database. Lecture Notes in Computer Science, 2018, , 83-100.	1.0	25
40	Towards secure and cost-effective fuzzy access control in mobile cloud computing. Soft Computing, 2017, 21, 2643-2649.	2.1	13
41	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
42	Towards Multi-user Searchable Encryption Supporting Boolean Query and Fast Decryption. Lecture Notes in Computer Science, 2017, , 24-38.	1.0	16
43	RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero. Lecture Notes in Computer Science, 2017, , 456-474.	1.0	157
44	Multi-user Cloud-Based Secure Keyword Search. Lecture Notes in Computer Science, 2017, , 227-247.	1.0	15
45	Attribute-Based Encryption with Expressive and Authorized Keyword Search. Lecture Notes in Computer Science, 2017, , 106-126.	1.0	11
46	Towards Revocable Fine-Grained Encryption of Cloud Data: Reducing Trust upon Cloud. Lecture Notes in Computer Science, 2017, , 127-144.	1.0	4
47	Privacy-Preserving Public Auditing Protocol for Low-Performance End Devices in Cloud. IEEE Transactions on Information Forensics and Security, 2016, 11, 2572-2583.	4.5	97
48	Trust Enhancement over Range Search for Encrypted Data. , 2016, , .		9
49	Trusted Boolean Search on Cloud Using Searchable Symmetric Encryption. , 2016, , .		16
50	A Trust and Privacy Preserving Handover Authentication Protocol for Wireless Networks. , 2016, , .		11
51	Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2016, 11, 1661-1673.	4.5	122
52	An Efficient Non-interactive Multi-client Searchable Encryption with Support for Boolean Queries. Lecture Notes in Computer Science, 2016, , 154-172.	1.0	85
53	Anonymous Announcement System (AAS) for Electric Vehicle in VANETs. Computer Journal, 2016, , .	1.5	1
54	Efficient Multi-Function Data Sharing and Searching Mechanism for Cloud-Based Encrypted Data. , 2016, , .		17

#	Article	IF	Citations
55	An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2016, 11, 1265-1277.	4.5	215
56	On Lightweight Security Enforcement in Cyber-Physical Systems. Lecture Notes in Computer Science, 2016, , 97-112.	1.0	14
57	Secret Picture: An Efficient Tool for Mitigating Deletion Delay on OSN. Lecture Notes in Computer Science, 2016, , 467-477.	1.0	1
58	Efficient Privacy-Preserving Charging Station Reservation System for Electric Vehicles. Computer Journal, 2016, 59, 1040-1053.	1.5	12
59	Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. IEEE Transactions on Information Forensics and Security, 2016, 11, 484-497.	4.5	85
60	Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing. Future Generation Computer Systems, 2016, 62, 190-195.	4.9	72
61	Cooperative attribute-based access control for enterprise computing system. International Journal of Embedded Systems, 2015, 7, 191.	0.2	7
62	PEVTS: Privacy-Preserving Electric Vehicles Test-Bedding Scheme. , 2015, , .		0
63	Lightweight Anonymous Authentication for AdÂHoc Group: A Ring Signature Approach. Lecture Notes in Computer Science, 2015, , 215-226.	1.0	12
64	Towards secure and reliable cloud storage against data re-outsourcing. Future Generation Computer Systems, 2015, 52, 86-94.	4.9	34
65	On the security of a lightweight authentication and encryption scheme for mobile ad hoc network. Security and Communication Networks, 2015, 8, 3094-3098.	1.0	2
66	Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1578-1589.	4.5	81
67	Universal designated verifier transitive signatures for graph-based big data. Information Sciences, 2015, 318, 144-156.	4.0	17
68	Privacy Concerns for Photo Sharing in Online Social Networks. IEEE Internet Computing, 2015, 19, 58-63.	3.2	33
69	Comments on 'Efficient Revocable Certificateless Encryption Secure in the Standard Model'. Computer Journal, 2015, 58, 779-781.	1.5	5
70	Secure sharing and searching for real-time video data in mobile cloud. IEEE Network, 2015, 29, 46-50.	4.9	57
71	Asymmetric Cross-cryptosystem Re-encryption Applicable to Efficient and Secure Mobile Access to Outsourced Data. , 2015, , .		11
72	Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. Computer Journal, 2015, 58, 2778-2792.	1.5	18

#	Article	IF	Citations
73	Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. Lecture Notes in Computer Science, 2015, , 146-166.	1.0	54
74	A New Public Remote Integrity Checking Scheme with User Privacy. Lecture Notes in Computer Science, 2015, , 377-394.	1.0	11
75	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
76	Cost-Effective Authentic and Anonymous Data Sharing with Forward Security. IEEE Transactions on Computers, 2015, 64, 971-983.	2.4	93
77	Time-Bound Anonymous Authentication for Roaming Networks. IEEE Transactions on Information Forensics and Security, 2015, 10, 178-189.	4.5	46
78	<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
79	Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. Future Generation Computer Systems, 2015, 52, 67-76.	4.9	190
80	A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid. IEEE Transactions on Cloud Computing, 2015, 3, 233-244.	3.1	199
81	Fully Secure Ciphertext-Policy Attribute Based Encryption with Security Mediator. Lecture Notes in Computer Science, 2015, , 274-289.	1.0	11
82	TIMER: Secure and Reliable Cloud Storage against Data Re-outsourcing. Lecture Notes in Computer Science, 2014, , 346-358.	1.0	15
83	An efficient PHR service system supporting fuzzy keyword search and fine-grained access control. Soft Computing, 2014, 18, 1795-1802.	2.1	51
84	A New Payment System for Enhancing Location Privacy of Electric Vehicles. IEEE Transactions on Vehicular Technology, 2014, 63, 3-18.	3.9	70
85	Improvements on an authentication scheme for vehicular sensor networks. Expert Systems With Applications, 2014, 41, 2559-2564.	4.4	106
86	Toward efficient and privacy-preserving computing in big data era. IEEE Network, 2014, 28, 46-50.	4.9	247
87	A secure remote data integrity checking cloud storage system from threshold encryption. Journal of Ambient Intelligence and Humanized Computing, 2014, 5, 857-865.	3.3	13
88	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
89	Linkable Ring Signature with Unconditional Anonymity. IEEE Transactions on Knowledge and Data Engineering, 2014, 26, 157-165.	4.0	68
90	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

#	Article	IF	Citations
91	Identity-Based Encryption with Post-Challenge Auxiliary Inputs for Secure Cloud Applications and Sensor Networks. Lecture Notes in Computer Science, 2014, , 130-147.	1.0	23
92	New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era. Lecture Notes in Computer Science, 2014, , 182-199.	1.0	5
93	Security Concerns in Popular Cloud Storage Services. IEEE Pervasive Computing, 2013, 12, 50-57.	1.1	61
94	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
95	Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. Theoretical Computer Science, 2013, 469, 1-14.	0.5	57
96	Comments on "Analysis and Improvement of a Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions". IEEE Communications Letters, 2013, 17, 1521-1523.	2.5	27
97	Privacy-preserving smart metering with regional statistics and personal enquiry services. , 2013, , .		19
98	Efficient Linkable and/or Threshold Ring Signature Without Random Oracles. Computer Journal, 2013, 56, 407-421.	1.5	41
99	Threshold-Oriented Optimistic Fair Exchange. Lecture Notes in Computer Science, 2013, , 424-438.	1.0	2
100	Towards Anonymous Ciphertext Indistinguishability with Identity Leakage. Lecture Notes in Computer Science, 2013, , 139-153.	1.0	5
101	Verifier-local revocation group signatures with time-bound keys. , 2012, , .		24
102	Forward Secure Attribute-Based Signatures. Lecture Notes in Computer Science, 2012, , 167-177.	1.0	7
103	Enhancing Location Privacy for Electric Vehicles (at the Right time). Lecture Notes in Computer Science, 2012, , 397-414.	1.0	28
104	Efficient Escrow-Free Identity-Based Signature. Lecture Notes in Computer Science, 2012, , 161-174.	1.0	6
105	Online/Offline Identity-Based Signcryption Revisited. Lecture Notes in Computer Science, 2011, , 36-51.	1.0	18
106	Identity-based online/offline key encapsulation and encryption. , 2011, , .		32
107	Short and Efficient Certificate-Based Signature. Lecture Notes in Computer Science, 2011, , 167-178.	1.0	12
108	Forward Secure Ring Signature without Random Oracles. Lecture Notes in Computer Science, 2011, , 1-14.	1.0	22

#	Article	IF	Citations
109	Threshold ring signature without random oracles. , 2011, , .		14
110	Identity-Based Server-Aided Decryption. Lecture Notes in Computer Science, 2011, , 337-352.	1.0	8
111	Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security, 2010, 9, 287-296.	2.3	117
112	Practical ID-based encryption for wireless sensor network. , 2010, , .		27
113	Short Generic Transformation to Strongly Unforgeable Signature in the Standard Model. Lecture Notes in Computer Science, 2010, , 168-181.	1.0	3
114	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
115	A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack. Lecture Notes in Computer Science, 2009, , 143-155.	1.0	8
116	Online/Offline Ring Signature Scheme. Lecture Notes in Computer Science, 2009, , 80-90.	1.0	7
117	Certificate-based sequential aggregate signature. , 2009, , .		94
118	Traceable and Retrievable Identity-Based Encryption. Lecture Notes in Computer Science, 2008, , 94-110.	1.0	26
119	Efficient Certificate-Based Encryption in the Standard Model. Lecture Notes in Computer Science, 2008, , 144-155.	1.0	20
120	Certificate-Based Signature Schemes without Pairings or Random Oracles. Lecture Notes in Computer Science, 2008, , 285-297.	1.0	37
121	Sanitizable Signatures Revisited. Lecture Notes in Computer Science, 2008, , 80-97.	1.0	13
122	Revocable Ring Signature. Journal of Computer Science and Technology, 2007, 22, 785-794.	0.9	48
123	Certificate Based (Linkable) Ring Signature. , 2007, , 79-92.		46
124	ENHANCED SECURITY MODELS AND A GENERIC CONSTRUCTION APPROACH FOR LINKABLE RING SIGNATURE. International Journal of Foundations of Computer Science, 2006, 17, 1403-1422.	0.8	23
125	Ring signatures without random oracles. , 2006, , .		63
126	Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature. Lecture Notes in Computer Science, 2006, , 364-378.	1.0	34

#	Article	IF	Citations
127	ID-Based Ring Signature Scheme Secure in the Standard Model. Lecture Notes in Computer Science, 2006, , 1-16.	1.0	48
128	Ring Signature with Designated Linkability. Lecture Notes in Computer Science, 2006, , 104-119.	1.0	15
129	Transferable E-Cash Revisit. IFIP Advances in Information and Communication Technology, 2005, , 171-188.	0.5	0
130	On the Security Models of (Threshold) Ring Signature Schemes. Lecture Notes in Computer Science, 2005, , 204-217.	1.0	25
131	A Restricted Multi-show Credential System and Its Application on E-Voting. Lecture Notes in Computer Science, 2005, , 268-279.	1.0	3
132	Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups. Lecture Notes in Computer Science, 2004, , 325-335.	1.0	238
133	Separable Linkable Threshold Ring Signatures. Lecture Notes in Computer Science, 2004, , 384-398.	1.0	71
134	A Separable Threshold Ring Signature Scheme. Lecture Notes in Computer Science, 2004, , 12-26.	1.0	45
135	On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST. Lecture Notes in Computer Science, 2003, , 34-46.	1.0	37