

Kaitai Liang

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/2801831/publications.pdf>

Version: 2024-02-01

88
papers

2,948
citations

185998

28
h-index

182168

51
g-index

90
all docs

90
docs citations

90
times ranked

2234
citing authors

| # | ARTICLE | IF | CITATIONS |
|----|---|-----|-----------|
| 1 | On-the-Fly Privacy for Location Histograms. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 566-578. | 3.7 | 4 |
| 2 | Efficient Encrypted Data Search With Expressive Queries and Flexible Update. IEEE Transactions on Services Computing, 2022, 15, 1619-1633. | 3.2 | 16 |
| 3 | ROSE: Robust Searchable Encryption With Forward and Backward Security. IEEE Transactions on Information Forensics and Security, 2022, 17, 1115-1130. | 4.5 | 16 |
| 4 | Encryption Switching Service: Securely Switch Your Encrypted Data to Another Format. IEEE Transactions on Services Computing, 2021, 14, 1357-1369. | 3.2 | 8 |
| 5 | Lightweight Searchable Encryption Protocol for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2021, 17, 4248-4259. | 7.2 | 49 |
| 6 | 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. | 0.2 | 1 |
| 7 | Improved Probabilistic Context-Free Grammars for Passwords Using Word Extraction. , 2021, , . | | 4 |
| 8 | 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. | 4.0 | 7 |
| 9 | Distributed additive encryption and quantization for privacy preserving federated deep learning. Neurocomputing, 2021, 463, 309-327. | 3.5 | 23 |
| 10 | Practical Threshold Multi-Factor Authentication. IEEE Transactions on Information Forensics and Security, 2021, 16, 3573-3588. | 4.5 | 11 |
| 11 | Searchchain: Blockchain-based private keyword search in decentralized storage. Future Generation Computer Systems, 2020, 107, 781-792. | 4.9 | 69 |
| 12 | Am I eclipsed? A smart detector of eclipse attacks for Ethereum. Computers and Security, 2020, 88, 101604. | 4.0 | 50 |
| 13 | SoProtector: Safeguard Privacy for Native SO Files in Evolving Mobile IoT Applications. IEEE Internet of Things Journal, 2020, 7, 2539-2552. | 5.5 | 16 |
| 14 | BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular <i>Ad Hoc</i> Networks. IEEE Transactions on Industrial Informatics, 2020, 16, 4146-4155. | 7.2 | 150 |
| 15 | Practical Attribute-Based Conjunctive Keyword Search Scheme. Computer Journal, 2020, 63, 1203-1215. | 1.5 | 2 |
| 16 | Dual Access Control for Cloud-Based Data Storage and Sharing. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1. | 3.7 | 23 |
| 17 | JSCSP: a Novel Policy-Based XSS Defense Mechanism for Browsers. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1. | 3.7 | 3 |
| 18 | Deep Binarized Convolutional Neural Network Inferences over Encrypted Data. , 2020, , . | | 2 |

| # | ARTICLE | IF | CITATIONS |
|----|--|-----|-----------|
| 19 | An Efficient Attribute-Based Multi-Keyword Search Scheme in Encrypted Keyword Generation. IEEE Access, 2020, 8, 99024-99036. | 2.6 | 11 |
| 20 | Trust2Privacy: A Novel Fuzzy Trust-to-Privacy Mechanism for Mobile Social Networks. IEEE Wireless Communications, 2020, 27, 72-78. | 6.6 | 29 |
| 21 | Privacy preserving search services against online attack. Computers and Security, 2020, 95, 101836. | 4.0 | 3 |
| 22 | A Security-Enhanced Certificateless Aggregate Signature Authentication Protocol for InVANETs. IEEE Network, 2020, 34, 22-29. | 4.9 | 25 |
| 23 | Post quantum proxy signature scheme based on the multivariate public key cryptographic signature. International Journal of Distributed Sensor Networks, 2020, 16, 155014772091477. | 1.3 | 4 |
| 24 | Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices. IEEE Systems Journal, 2019, 13, 2775-2785. | 2.9 | 59 |
| 25 | Passive Attacks Against Searchable Encryption. IEEE Transactions on Information Forensics and Security, 2019, 14, 789-802. | 4.5 | 77 |
| 26 | Efficient Attribute-Based Data Sharing Scheme with Hidden Access Structures. Computer Journal, 2019, 62, 1748-1760. | 1.5 | 7 |
| 27 | Toward Practical Privacy-Preserving Processing Over Encrypted Data in IoT: An Assistive Healthcare Use Case. IEEE Internet of Things Journal, 2019, 6, 10177-10190. | 5.5 | 41 |
| 28 | Secure Edge Computing with Lightweight Control-Flow Property-based Attestation. , 2019, , . | | 13 |
| 29 | Fine-grained information flow control using attributes. Information Sciences, 2019, 484, 167-182. | 4.0 | 13 |
| 30 | TAW: Cost-Effective Threshold Authentication With Weights for Internet of Things. IEEE Access, 2019, 7, 30112-30125. | 2.6 | 6 |
| 31 | An efficient blind filter: Location privacy protection and the access control in FinTech. Future Generation Computer Systems, 2019, 100, 797-810. | 4.9 | 12 |
| 32 | A Behavior Based Trustworthy Service Composition Discovery Approach in Cloud Environment. IEEE Access, 2019, 7, 56492-56503. | 2.6 | 13 |
| 33 | Polynomial-based modifiable blockchain structure for removing fraud transactions. Future Generation Computer Systems, 2019, 99, 154-163. | 4.9 | 20 |
| 34 | A New Encrypted Data Switching Protocol: Bridging IBE and ABE Without Loss of Data Confidentiality. IEEE Access, 2019, 7, 50658-50668. | 2.6 | 2 |
| 35 | Quantum-Resistant Identity-Based Signature with Message Recovery and Proxy Delegation. Symmetry, 2019, 11, 272. | 1.1 | 3 |
| 36 | CCA Secure Public Key Encryption against After-the-Fact Leakage without NIZK Proofs. Security and Communication Networks, 2019, 2019, 1-8. | 1.0 | 1 |

| # | ARTICLE | IF | CITATIONS |
|----|--|-----|-----------|
| 37 | Using Sparse Representation to Detect Anomalies in Complex WSNs. ACM Transactions on Intelligent Systems and Technology, 2019, 10, 1-18. | 2.9 | 9 |
| 38 | DT-CP: A Double-TTPs-Based Contract-Signing Protocol With Lower Computational Cost. IEEE Access, 2019, 7, 174740-174749. | 2.6 | 14 |
| 39 | A blockchain-based location privacy-preserving crowdsensing system. Future Generation Computer Systems, 2019, 94, 408-418. | 4.9 | 128 |
| 40 | 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 Hsueh K'an, 2019, 42, 80-86. | 0.6 | 4 |
| 41 | CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage. IEEE Transactions on Services Computing, 2019, , 1-1. | 3.2 | 33 |
| 42 | Cryptanalysis of Raindrop and FBC. Lecture Notes in Computer Science, 2019, , 536-551. | 1.0 | 3 |
| 43 | Certificateless Public Key Authenticated Encryption With Keyword Search for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2018, 14, 3618-3627. | 7.2 | 155 |
| 44 | 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 |
| 45 | Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat. Future Generation Computer Systems, 2018, 79, 337-349. | 4.9 | 32 |
| 46 | Expressive attribute-based keyword search with constant-size ciphertext. Soft Computing, 2018, 22, 5163-5177. | 2.1 | 18 |
| 47 | Auditable Σ -Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2018, 13, 94-105. | 4.5 | 157 |
| 48 | Message Integration Authentication in the Internet-of-Things via Lattice-Based Batch Signatures. Sensors, 2018, 18, 4056. | 2.1 | 4 |
| 49 | Delegation of Decryption Rights With Revocability From Learning With Errors. IEEE Access, 2018, 6, 61163-61175. | 2.6 | 2 |
| 50 | Time-Based Direct Revocable Ciphertext-Policy Attribute-Based Encryption with Short Revocation List. Lecture Notes in Computer Science, 2018, , 516-534. | 1.0 | 54 |
| 51 | DABEHR: Decentralized Attribute-Based Electronic Health Record System with Constant-Size Storage Complexity. Lecture Notes in Computer Science, 2017, , 611-626. | 1.0 | 3 |
| 52 | An Efficient Key-Policy Attribute-Based Searchable Encryption in Prime-Order Groups. Lecture Notes in Computer Science, 2017, , 39-56. | 1.0 | 7 |
| 53 | Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation. Computer Journal, 2017, 60, 1210-1222. | 1.5 | 22 |
| 54 | Cost-effective privacy-preserving vehicular urban sensing system. Personal and Ubiquitous Computing, 2017, 21, 893-901. | 1.9 | 6 |

| # | ARTICLE | IF | CITATIONS |
|----|--|-----|-----------|
| 55 | One-Round Attribute-Based Key Exchange in the Multi-Party Setting. International Journal of Foundations of Computer Science, 2017, 28, 725-742. | 0.8 | 3 |
| 56 | Hierarchical Conditional Proxy Re-Encryption: A New Insight of Fine-Grained Secure Data Sharing. Lecture Notes in Computer Science, 2017, , 118-135. | 1.0 | 1 |
| 57 | A Modified Segmentation Approach for Overlapping Elliptical Objects with Various Sizes. Lecture Notes in Computer Science, 2017, , 222-236. | 1.0 | 0 |
| 58 | A Cloud-Based Access Control Scheme with User Revocation and Attribute Update. Lecture Notes in Computer Science, 2016, , 525-540. | 1.0 | 26 |
| 59 | A data hiding approach for sensitive smartphone data. , 2016, , . | | 10 |
| 60 | Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security, 2016, 11, 1661-1673. | 4.5 | 122 |
| 61 | Online/Offline Public-Index Predicate Encryption for Fine-Grained Mobile Access Control. Lecture Notes in Computer Science, 2016, , 588-605. | 1.0 | 3 |
| 62 | One-Round Attribute-Based Key Exchange in the Multi-party Setting. Lecture Notes in Computer Science, 2016, , 227-243. | 1.0 | 2 |
| 63 | Efficient Multi-Function Data Sharing and Searching Mechanism for Cloud-Based Encrypted Data. , 2016, , . | | 17 |
| 64 | Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data. IEEE Transactions on Information Forensics and Security, 2016, 11, 2365-2376. | 4.5 | 47 |
| 65 | Anonymous Proxy Signature with Hierarchical Traceability: TABLE 1.. Computer Journal, 2016, 59, 559-569. | 1.5 | 3 |
| 66 | Secret Picture: An Efficient Tool for Mitigating Deletion Delay on OSN. Lecture Notes in Computer Science, 2016, , 467-477. | 1.0 | 1 |
| 67 | Two-Factor Data Security Protection Mechanism for Cloud Storage System. IEEE Transactions on Computers, 2016, 65, 1992-2004. | 2.4 | 56 |
| 68 | Secure bidirectional proxy re-encryption for cryptographic cloud storage. Pervasive and Mobile Computing, 2016, 28, 113-121. | 2.1 | 26 |
| 69 | Broadcast encryption with dealership. International Journal of Information Security, 2016, 15, 271-283. | 2.3 | 8 |
| 70 | Secure and Traceable Framework for Data Circulation. Lecture Notes in Computer Science, 2016, , 376-388. | 1.0 | 0 |
| 71 | A New Transitive Signature Scheme. Lecture Notes in Computer Science, 2016, , 156-167. | 1.0 | 2 |
| 72 | A new unpredictability-based radio frequency identification forward privacy model and a provably secure construction. Security and Communication Networks, 2015, 8, 2836-2849. | 1.0 | 2 |

| # | ARTICLE | IF | CITATIONS |
|----|--|-----|-----------|
| 73 | 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 |
| 74 | Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. IEEE Transactions on Information Forensics and Security, 2015, 10, 1578-1589. | 4.5 | 81 |
| 75 | Privacy Concerns for Photo Sharing in Online Social Networks. IEEE Internet Computing, 2015, 19, 58-63. | 3.2 | 33 |
| 76 | Secure sharing and searching for real-time video data in mobile cloud. IEEE Network, 2015, 29, 46-50. | 4.9 | 57 |
| 77 | Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. Computer Journal, 2015, 58, 2778-2792. | 1.5 | 18 |
| 78 | Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. Lecture Notes in Computer Science, 2015, , 146-166. | 1.0 | 54 |
| 79 | 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 |
| 80 | Cost-Effective Authentic and Anonymous Data Sharing with Forward Security. IEEE Transactions on Computers, 2015, 64, 971-983. | 2.4 | 93 |
| 81 | A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds. Concurrency Computation Practice and Experience, 2015, 27, 2004-2027. | 1.4 | 22 |
| 82 | Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts. Theoretical Computer Science, 2014, 539, 87-105. | 0.5 | 47 |
| 83 | 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 |
| 84 | 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 |
| 85 | 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 |
| 86 | A Ciphertext-Policy Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security. , 2013, , . | | 85 |
| 87 | A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles. Lecture Notes in Computer Science, 2013, , 231-246. | 1.0 | 24 |
| 88 | A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release. Lecture Notes in Computer Science, 2013, , 132-146. | 1.0 | 20 |