

# Mingwu Zhang

## List of Publications by Citations

**Source:** <https://exaly.com/author-pdf/1701896/mingwu-zhang-publications-by-citations.pdf>

**Version:** 2024-04-26

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

92  
papers

955  
citations

18  
h-index

27  
g-index

98  
ext. papers

1,248  
ext. citations

2.8  
avg, IF

5.31  
L-index

#	Paper	IF	Citations
92	Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization. <i>IEEE Transactions on Information Forensics and Security</i> , <b>2015</b> , 10, 458-470	8	108
91	Efficient Privacy-Preserving Cube-Data Aggregation Scheme for Smart Grids. <i>IEEE Transactions on Information Forensics and Security</i> , <b>2017</b> , 12, 1369-1381	8	75
90	Public Key Encryption with Delegated Equality Test in a Multi-User Setting. <i>Computer Journal</i> , <b>2015</b> , 58, 986-1002	1.3	64
89	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. <i>IEEE Internet of Things Journal</i> , <b>2020</b> , 7, 10660-10672	10.7	58
88	On the Soundness and Security of Privacy-Preserving SVM for Outsourcing Data Classification. <i>IEEE Transactions on Dependable and Secure Computing</i> , <b>2018</b> , 15, 906-912	3.9	42
87	Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation. <i>Science China Information Sciences</i> , <b>2018</b> , 61, 1	3.4	29
86	Efficient Identity-Based Signcryption Scheme for Multiple Receivers. <i>Lecture Notes in Computer Science</i> , <b>2007</b> , 13-21	0.9	28
85	An ID-based cryptographic mechanisms based on GDLP and IFP. <i>Information Processing Letters</i> , <b>2012</b> , 112, 753-758	0.8	27
84	. <i>IEEE Systems Journal</i> , <b>2019</b> , 13, 1478-1486	4.3	26
83	An efficient aggregation scheme resisting on malicious data mining attacks for smart grid. <i>Information Sciences</i> , <b>2020</b> , 526, 289-300	7.7	26
82	Accountable mobile E-commerce scheme in intelligent cloud system transactions. <i>Journal of Ambient Intelligence and Humanized Computing</i> , <b>2018</b> , 9, 1889-1899	3.7	26
81	Bounded Leakage-Resilient Functional Encryption with Hidden Vector Predicate. <i>Computer Journal</i> , <b>2013</b> , 56, 464-477	1.3	24
80	SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems. <i>IEEE Systems Journal</i> , <b>2021</b> , 15, 2980-2988	4.3	24
79	Efficient Constructions of Anonymous Multireceiver Encryption Protocol and Their Deployment in Group E-mail Systems With Privacy Preservation. <i>IEEE Systems Journal</i> , <b>2013</b> , 7, 410-419	4.3	23
78	A cloud-aided privacy-preserving multi-dimensional data comparison protocol. <i>Information Sciences</i> , <b>2021</b> , 545, 739-752	7.7	22
77	A Privacy-Preserving Optimization of Neighborhood-Based Recommendation for Medical-Aided Diagnosis and Treatment. <i>IEEE Internet of Things Journal</i> , <b>2021</b> , 8, 10830-10842	10.7	21
76	An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection. <i>Computer Journal</i> , <b>2018</b> , 61, 526-538	1.3	19

75	After-the-Fact Leakage-Resilient Identity-Based Authenticated Key Exchange. <i>IEEE Systems Journal</i> , <b>2018</b> , 12, 2017-2026	4.3	19
74	Realizing secret sharing with general access structure. <i>Information Sciences</i> , <b>2016</b> , 367-368, 209-220	7.7	15
73	A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme. <i>IEEE Internet of Things Journal</i> , <b>2020</b> , 7, 3083-3093	10.7	14
72	A Secure Clinical Diagnosis With Privacy-Preserving Multiclass Support Vector Machine in Clouds. <i>IEEE Systems Journal</i> , <b>2020</b> , 1-12	4.3	14
71	Identity-based partially blind signature in the standard model for electronic cash. <i>Mathematical and Computer Modelling</i> , <b>2013</b> , 58, 196-203		13
70	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. <i>IEEE Systems Journal</i> , <b>2017</b> , 11, 1018-1026	4.3	12
69	Privacy-preserving Quantum Sealed-bid Auction Based on Grover's Search Algorithm. <i>Scientific Reports</i> , <b>2019</b> , 9, 7626	4.9	12
68	Security analysis of a homomorphic signature scheme for network coding. <i>Security and Communication Networks</i> , <b>2015</b> , 8, 4053-4060	1.9	11
67	Efficient Secret Authenticatable Anonymous Signcryption Scheme with Identity Privacy. <i>Lecture Notes in Computer Science</i> , <b>2008</b> , 126-137	0.9	11
66	PPO-DFK: A Privacy-Preserving Optimization of Distributed Fractional Knapsack With Application in Secure Footballer Configurations. <i>IEEE Systems Journal</i> , <b>2021</b> , 15, 759-770	4.3	11
65	Provably Leakage-Resilient Password-Based Authenticated Key Exchange in the Standard Model. <i>IEEE Access</i> , <b>2017</b> , 5, 26832-26841	3.5	9
64	Efficient and adaptively secure broadcast encryption systems. <i>Security and Communication Networks</i> , <b>2013</b> , 6, 1044-1052	1.9	8
63	. <i>IEEE Access</i> , <b>2019</b> , 7, 72105-72112	3.5	7
62	Obfuscating Re-encryption Algorithm With Flexible and Controllable Multi-Hop on Untrusted Outsourcing Server. <i>IEEE Access</i> , <b>2017</b> , 5, 26419-26434	3.5	7
61	A Novel Privacy-Preserving Authentication Scheme for V2G Networks. <i>IEEE Systems Journal</i> , <b>2020</b> , 14, 1963-1971	4.3	7
60	Functional Encryption Resilient to Hard-to-Invert Leakage. <i>Computer Journal</i> , <b>2015</b> , 58, 735-749	1.3	6
59	Tolerating Sensitive-Leakage With Larger Plaintext-Space and Higher Leakage-Rate in Privacy-Aware Internet-of-Things. <i>IEEE Access</i> , <b>2018</b> , 6, 33859-33870	3.5	6
58	Anonymous spatial encryption under affine space delegation functionality with full security. <i>Information Sciences</i> , <b>2014</b> , 277, 715-730	7.7	6

57	A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. <i>Frontiers of Computer Science</i> , <b>2020</b> , 14, 1	2.2	6
56	Cryptanalysis and Improvement of Quantum Sealed-Bid Auction. <i>International Journal of Theoretical Physics</i> , <b>2020</b> , 59, 1917-1926	1.1	6
55	An efficient and adaptive data-hiding scheme based on secure random matrix. <i>PLoS ONE</i> , <b>2019</b> , 14, e0223892	3.9	5
54	Privacy-friendly weighted-reputation aggregation protocols against malicious adversaries in cloud services. <i>International Journal of Communication Systems</i> , <b>2016</b> , 29, 1863-1872	1.7	5
53	Quantum Secure Multi-party Private Set Intersection Cardinality. <i>International Journal of Theoretical Physics</i> , <b>2020</b> , 59, 1992-2007	1.1	5
52	Group-oriented setting $\bar{\eta}$ multisigncryption scheme with threshold designcryption. <i>Information Sciences</i> , <b>2011</b> , 181, 4041-4050	7.7	5
51	Improved Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. <i>IEEE Systems Journal</i> , <b>2021</b> , 1-9	4.3	5
50	Token-Leakage Tolerant and Vector Obfuscated IPE and Application in Privacy-Preserving Two-Party Point/Polynomial Evaluations. <i>Computer Journal</i> , <b>2016</b> , 59, 493-507	1.3	4
49	Reconciling and improving of multi-receiver signcryption protocols with threshold decryption. <i>Security and Communication Networks</i> , <b>2012</b> , 5, 1430-1440	1.9	4
48	Anonymous Encryption with Partial-Order Subset Delegation Functionality. <i>Lecture Notes in Computer Science</i> , <b>2011</b> , 154-169	0.9	4
47	LR-UESDE: A Continual-Leakage Resilient Encryption with Unbounded Extensible Set Delegation. <i>Lecture Notes in Computer Science</i> , <b>2012</b> , 125-142	0.9	4
46	PPDDS: A Privacy-Preserving Disease Diagnosis Scheme Based on the Secure Mahalanobis Distance Evaluation Model. <i>IEEE Systems Journal</i> , <b>2021</b> , 1-11	4.3	4
45	Verifiable Quantum Key Exchange with Authentication. <i>International Journal of Theoretical Physics</i> , <b>2021</b> , 60, 227-242	1.1	4
44	Privacy-Preserving Federated Learning in Medical Diagnosis with Homomorphic Re-Encryption. <i>Computer Standards and Interfaces</i> , <b>2021</b> , 103583	3.5	4
43	Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks. <i>IEEE Systems Journal</i> , <b>2020</b> , 14, 5320-5328	4.3	3
42	LR-FEAD: leakage-tolerating and attribute-hiding functional encryption mechanism with delegation in affine subspaces. <i>Journal of Supercomputing</i> , <b>2014</b> , 70, 1405-1432	2.5	3
41	An efficient fair UC-secure protocol for two-party computation. <i>Security and Communication Networks</i> , <b>2014</b> , 7, 1253-1263	1.9	3
40	Program Obfuscator for Privacy-Carrying Unidirectional One-hop Re-encryption. <i>Lecture Notes in Computer Science</i> , <b>2015</b> , 133-142	0.9	3

39	GeoEnc: Geometric Area Based Keys and Policies in Functional Encryption Systems. <i>Lecture Notes in Computer Science</i> , <b>2011</b> , 241-258	0.9	3
38	Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing. <i>Theoretical Computer Science</i> , <b>2021</b> , 860, 1-22	1.1	3
37	Novel Public-Key Encryption with Continuous Leakage Amplification. <i>Computer Journal</i> , <b>2021</b> , 64, 1163-1177	1.7	3
36	. <i>IEEE Access</i> , <b>2018</b> , 6, 43936-43945	3.5	3
35	A robust, distributed, and privacy-preserving aggregation scheme for smart grid communications <b>2019</b> , 42, 54-65		2
34	Insecurity of an Efficient Identity-Based Proxy Signature in the Standard Model. <i>Computer Journal</i> , <b>2015</b> , 58, 2507-2508	1.3	2
33	Key continual-leakage resilient broadcast cryptosystem from dual system in broadcast networks. <i>Frontiers of Computer Science</i> , <b>2014</b> , 8, 456-468	2.2	2
32	Leakage-Resilient Password-Based Authenticated Key Exchange. <i>Lecture Notes in Computer Science</i> , <b>2017</b> , 285-296	0.9	2
31	Continuous Leakage Resilient Lossy Trapdoor Functions. <i>Information (Switzerland)</i> , <b>2017</b> , 8, 38	2.6	2
30	Secure and Efficient Certificate-Based Proxy Signature Schemes for Industrial Internet of Things. <i>IEEE Systems Journal</i> , <b>2021</b> , 1-12	4.3	2
29	Strongly average-case secure obfuscation: achieving input privacy and circuit obscurity. <i>Security and Communication Networks</i> , <b>2016</b> , 9, 1737-1747	1.9	2
28	PP-OCQ: A distributed privacy-preserving optimal closeness query scheme for social networks. <i>Computer Standards and Interfaces</i> , <b>2021</b> , 74, 103484	3.5	2
27	Secure and Membership-Based Data Sharing Scheme in V2G Networks. <i>IEEE Access</i> , <b>2018</b> , 6, 58450-58460	3.5	2
26	Quantum private set intersection cardinality based on bloom filter. <i>Scientific Reports</i> , <b>2021</b> , 11, 17332	4.9	2
25	An error-tolerant keyword search scheme based on public-key encryption in secure cloud computing. <i>Concurrency Computation Practice and Experience</i> , <b>2016</b> , 28, 1083-1093	1.4	1
24	Strong Privacy-preserving Two-party Scalar Product Quantum Protocol. <i>International Journal of Theoretical Physics</i> , <b>2019</b> , 58, 4249-4257	1.1	1
23	Anonymous encryption with partial-order subset delegation and its application in privacy email systems. <i>IET Information Security</i> , <b>2014</b> , 8, 240-249	1.4	1
22	PPGJ: A privacy-preserving general join for outsourced encrypted database. <i>Security and Communication Networks</i> , <b>2014</b> , 7, 1232-1244	1.9	1

21	Efficient signcryption in the standard model. <i>Concurrency Computation Practice and Experience</i> , <b>2012</b> , 24, 1977-1989	1.4	1
20	PRIVACY-PRESERVING OLAP FOR ACCURATE ANSWER. <i>Journal of Circuits, Systems and Computers</i> , <b>2012</b> , 21, 1250009	0.9	1
19	Analysis and Improvement of a Secret Broadcast with Binding Encryption in Broadcasting Networks. <i>IEICE Transactions on Information and Systems</i> , <b>2012</b> , E95-D, 686-689	0.6	1
18	Cryptanalysis of Strong Designated Verifier Signature Scheme with Non-delegatability and Non-transferability. <i>IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences</i> , <b>2012</b> , E95-A, 259-262	0.4	1
17	An Efficient Leakage-Resilient Authenticated Group Key Exchange Protocol. <i>Lecture Notes in Computer Science</i> , <b>2019</b> , 665-674	0.9	1
16	Updatable Lossy Trapdoor Functions Under Consecutive Leakage. <i>Computer Journal</i> , <b>2020</b> , 63, 648-656	1.3	1
15	PP-VCA: A Privacy-Preserving and Verifiable Combinatorial Auction Mechanism. <i>Wireless Communications and Mobile Computing</i> , <b>2020</b> , 2020, 1-11	1.9	1
14	. <i>IEEE Access</i> , <b>2021</b> , 9, 70616-70627	3.5	1
13	Anonymous quantum voting protocol based on Chinese remainder theorem. <i>European Physical Journal D</i> , <b>2021</b> , 75, 1	1.3	1
12	Privacy-Enhanced Mean-Variance Scheme Against Malicious Signature Attacks in Smart Grids. <i>Communications in Computer and Information Science</i> , <b>2022</b> , 145-158	0.3	1
11	Measurement-device-independent quantum secure multiparty summation. <i>Quantum Information Processing</i> , <b>2022</b> , 21, 1	1.6	1
10	Unbounded anonymous hierarchical IBE with continual-key-leakage tolerance. <i>Security and Communication Networks</i> , <b>2014</b> , 7, 1974-1987	1.9	0
9	TPM-Based Conditional Privacy-Preserving Authentication Protocol in VANETs. <i>Symmetry</i> , <b>2022</b> , 14, 1123	1.7	0
8	Generic Constructions and Transformations of Decryption Consistent Encryption. <i>IETE Journal of Research</i> , <b>2014</b> , 60, 218-228	0.9	
7	Revisits and Transformations Among Functional Encryption Systems. <i>IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)</i> , <b>2014</b> , 31, 103-114	1.5	
6	Fully secure constructions of spatial encryption with vector privacy. <i>International Journal of Communication Systems</i> , <b>2014</b> , 27, 4307-4327	1.7	
5	Secure two-party integer comparison protocol without any third party. <i>Quantum Information Processing</i> , <b>2021</b> , 20, 1	1.6	
4	A Fair (t, n)-Threshold Secret Sharing Scheme with Efficient Cheater Identifying. <i>IFIP Advances in Information and Communication Technology</i> , <b>2019</b> , 122-132	0.5	

- 3 A Fair and Efficient Secret Sharing Scheme Based on Cloud Assisting. *Lecture Notes in Computer Science*, **2019**, 348-360 0.9
- 2 Cloud-Based Data-Sharing Scheme Using Verifiable and CCA-Secure Re-encryption from Indistinguishability Obfuscation. *Lecture Notes in Computer Science*, **2019**, 240-259 0.9
- 1 A Distributed and Privacy-Preserving Random Forest Evaluation Scheme with Fine Grained Access Control. *Symmetry*, **2022**, 14, 415 2.7