

# Mingwu Zhang

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/1701896/publications.pdf>

Version: 2024-02-01

95  
papers

1,596  
citations

304602

22  
h-index

345118

36  
g-index

98  
all docs

98  
docs citations

98  
times ranked

1024  
citing authors

#	ARTICLE	IF	CITATIONS
1	Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization. IEEE Transactions on Information Forensics and Security, 2015, 10, 458-470.	4.5	155
2	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. IEEE Internet of Things Journal, 2020, 7, 10660-10672.	5.5	109
3	Efficient Privacy-Preserving Cube-Data Aggregation Scheme for Smart Grids. IEEE Transactions on Information Forensics and Security, 2017, 12, 1369-1381.	4.5	104
4	A Privacy-Preserving Optimization of Neighborhood-Based Recommendation for Medical-Aided Diagnosis and Treatment. IEEE Internet of Things Journal, 2021, 8, 10830-10842.	5.5	98
5	Public Key Encryption with Delegated Equality Test in a Multi-User Setting. Computer Journal, 2015, 58, 986-1002.	1.5	84
6	An efficient aggregation scheme resisting on malicious data mining attacks for smart grid. Information Sciences, 2020, 526, 289-300.	4.0	54
7	On the Soundness and Security of Privacy-Preserving SVM for Outsourcing Data Classification. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 906-912.	3.7	53
8	A Secure Clinical Diagnosis With Privacy-Preserving Multiclass Support Vector Machine in Clouds. IEEE Systems Journal, 2022, 16, 67-78.	2.9	45
9	An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection. Computer Journal, 2018, 61, 526-538.	1.5	44
10	SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems. IEEE Systems Journal, 2021, 15, 2980-2988.	2.9	41
11	A cloud-aided privacy-preserving multi-dimensional data comparison protocol. Information Sciences, 2021, 545, 739-752.	4.0	36
12	Efficient Identity-Based Signcryption Scheme for Multiple Receivers. Lecture Notes in Computer Science, 2007, , 13-21.	1.0	35
13	Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation. Science China Information Sciences, 2018, 61, 1.	2.7	34
14	Obfuscating EVES Algorithm and Its Application in Fair Electronic Transactions in Public Clouds. IEEE Systems Journal, 2019, 13, 1478-1486.	2.9	32
15	An ID-based cryptographic mechanisms based on GDLP and IFP. Information Processing Letters, 2012, 112, 753-758.	0.4	30
16	Efficient Constructions of Anonymous Multireceiver Encryption Protocol and Their Deployment in Group E-mail Systems With Privacy Preservation. IEEE Systems Journal, 2013, 7, 410-419.	2.9	29
17	Accountable mobile E-commerce scheme in intelligent cloud system transactions. Journal of Ambient Intelligence and Humanized Computing, 2018, 9, 1889-1899.	3.3	29
18	A Novel Privacy-Preserving Authentication Scheme for V2G Networks. IEEE Systems Journal, 2020, 14, 1963-1971.	2.9	29

#	ARTICLE	IF	CITATIONS
19	Improved Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. <i>IEEE Systems Journal</i> , 2022, 16, 1842-1850.	2.9	28
20	Bounded Leakage-Resilient Functional Encryption with Hidden Vector Predicate. <i>Computer Journal</i> , 2013, 56, 464-477.	1.5	26
21	A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme. <i>IEEE Internet of Things Journal</i> , 2020, 7, 3083-3093.	5.5	26
22	Privacy-Preserving federated learning in medical diagnosis with homomorphic re-Encryption. <i>Computer Standards and Interfaces</i> , 2022, 80, 103583.	3.8	26
23	After-the-Fact Leakage-Resilient Identity-Based Authenticated Key Exchange. <i>IEEE Systems Journal</i> , 2018, 12, 2017-2026.	2.9	23
24	Realizing secret sharing with general access structure. <i>Information Sciences</i> , 2016, 367-368, 209-220.	4.0	18
25	Privacy-preserving Quantum Sealed-bid Auction Based on Grover's Search Algorithm. <i>Scientific Reports</i> , 2019, 9, 7626.	1.6	18
26	PPO-DFK: A Privacy-Preserving Optimization of Distributed Fractional Knapsack With Application in Secure Footballer Configurations. <i>IEEE Systems Journal</i> , 2021, 15, 759-770.	2.9	18
27	A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. <i>Frontiers of Computer Science</i> , 2020, 14, 1.	1.6	15
28	PPDDS: A Privacy-Preserving Disease Diagnosis Scheme Based on the Secure Mahalanobis Distance Evaluation Model. <i>IEEE Systems Journal</i> , 2022, 16, 4552-4562.	2.9	15
29	Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing. <i>Theoretical Computer Science</i> , 2021, 860, 1-22.	0.5	15
30	Efficient Secret Authenticatable Anonymous Signcryption Scheme with Identity Privacy. <i>Lecture Notes in Computer Science</i> , 2008, , 126-137.	1.0	15
31	Identity-based partially blind signature in the standard model for electronic cash. <i>Mathematical and Computer Modelling</i> , 2013, 58, 196-203.	2.0	13
32	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. <i>IEEE Systems Journal</i> , 2017, 11, 1018-1026.	2.9	13
33	A Feasible Quantum Protocol for Private Set Intersection Cardinality. <i>IEEE Access</i> , 2019, 7, 72105-72112.	2.6	13
34	Secure and Efficient Certificate-Based Proxy Signature Schemes for Industrial Internet of Things. <i>IEEE Systems Journal</i> , 2022, 16, 4719-4730.	2.9	12
35	Security analysis of a homomorphic signature scheme for network coding. <i>Security and Communication Networks</i> , 2015, 8, 4053-4060.	1.0	11
36	Tolerating Sensitive-Leakage With Larger Plaintext-Space and Higher Leakage-Rate in Privacy-Aware Internet-of-Things. <i>IEEE Access</i> , 2018, 6, 33859-33870.	2.6	11

#	ARTICLE	IF	CITATIONS
37	Provably Leakage-Resilient Password-Based Authenticated Key Exchange in the Standard Model. IEEE Access, 2017, 5, 26832-26841.	2.6	10
38	Quantum Secure Multi-party Private Set Intersection Cardinality. International Journal of Theoretical Physics, 2020, 59, 1992-2007.	0.5	10
39	SSBAS-FA: A secure sealed-bid e-auction scheme with fair arbitration based on time-released blockchain. Journal of Systems Architecture, 2022, 129, 102619.	2.5	10
40	PP-OCQ: A distributed privacy-preserving optimal closeness query scheme for social networks. Computer Standards and Interfaces, 2021, 74, 103484.	3.8	9
41	Novel Public-Key Encryption with Continuous Leakage Amplification. Computer Journal, 2021, 64, 1163-1177.	1.5	9
42	Efficient and adaptively secure broadcast encryption systems. Security and Communication Networks, 2013, 6, 1044-1052.	1.0	8
43	Obfuscating Re-encryption Algorithm With Flexible and Controllable Multi-Hop on Untrusted Outsourcing Server. IEEE Access, 2017, 5, 26419-26434.	2.6	8
44	Functional Encryption Resilient to Hard-to-Invert Leakage. Computer Journal, 2015, 58, 735-749.	1.5	7
45	Privacy-friendly weighted reputation aggregation protocols against malicious adversaries in cloud services. International Journal of Communication Systems, 2016, 29, 1863-1872.	1.6	7
46	Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks. IEEE Systems Journal, 2020, 14, 5320-5328.	2.9	7
47	Cryptanalysis and Improvement of Quantum Sealed-Bid Auction. International Journal of Theoretical Physics, 2020, 59, 1917-1926.	0.5	7
48	Verifiable Quantum Key Exchange with Authentication. International Journal of Theoretical Physics, 2021, 60, 227-242.	0.5	7
49	Anonymous quantum voting protocol based on Chinese remainder theorem. European Physical Journal D, 2021, 75, 1.	0.6	7
50	Quantum private set intersection cardinality based on bloom filter. Scientific Reports, 2021, 11, 17332.	1.6	7
51	Measurement-device-independent quantum secure multiparty summation. Quantum Information Processing, 2022, 21, 1.	1.0	7
52	TPM-Based Conditional Privacy-Preserving Authentication Protocol in VANETs. Symmetry, 2022, 14, 1123.	1.1	7
53	Group-oriented setting's multisigncryption scheme with threshold designcryption. Information Sciences, 2011, 181, 4041-4050.	4.0	6
54	Anonymous spatial encryption under affine space delegation functionality with full security. Information Sciences, 2014, 277, 715-730.	4.0	6

#	ARTICLE	IF	CITATIONS
55	An efficient and adaptive data-hiding scheme based on secure random matrix. PLoS ONE, 2019, 14, e0222892.	1.1	6
56	Efficient and Privacy-Preserving Massive Data Processing for Smart Grids. IEEE Access, 2021, 9, 70616-70627.	2.6	6
57	Token-Leakage Tolerant and Vector Obfuscated IPE and Application in Privacy-Preserving Two-Party Point/Polynomial Evaluations. Computer Journal, 2016, 59, 493-507.	1.5	5
58	A robust, distributed, and privacy-preserving aggregation scheme for smart grid communications. 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, 54-65.	0.6	5
59	An Efficient Identity Authentication Scheme With Provable Security and Anonymity for Mobile Edge Computing. IEEE Systems Journal, 2023, 17, 1012-1023.	2.9	5
60	Reconciling and improving of multi-receiver signcryption protocols with threshold decryption. Security and Communication Networks, 2012, 5, 1430-1440.	1.0	4
61	An efficient fair UC-secure protocol for two-party computation. Security and Communication Networks, 2014, 7, 1253-1263.	1.0	4
62	Continuous Leakage Resilient Lossy Trapdoor Functions. Information (Switzerland), 2017, 8, 38.	1.7	4
63	Consecutive Leakage-Resilient and Updatable Lossy Trapdoor Functions and Application in Sensitive Big-Data Environments. IEEE Access, 2018, 6, 43936-43945.	2.6	4
64	Secure and Membership-Based Data Sharing Scheme in V2G Networks. IEEE Access, 2018, 6, 58450-58460.	2.6	4
65	Anonymous Encryption with Partial-Order Subset Delegation Functionality. Lecture Notes in Computer Science, 2011, , 154-169.	1.0	4
66	LR-UESDE: A Continual-Leakage Resilient Encryption with Unbounded Extensible Set Delegation. Lecture Notes in Computer Science, 2012, , 125-142.	1.0	4
67	PPGJ: A privacy-preserving general join for outsourced encrypted database. Security and Communication Networks, 2014, 7, 1232-1244.	1.0	3
68	LR-FEAD: leakage-tolerating and attribute-hiding functional encryption mechanism with delegation in affine subspaces. Journal of Supercomputing, 2014, 70, 1405-1432.	2.4	3
69	An error-tolerant keyword search scheme based on public-key encryption in secure cloud computing. Concurrency Computation Practice and Experience, 2016, 28, 1083-1093.	1.4	3
70	Strong Privacy-preserving Two-party Scalar Product Quantum Protocol. International Journal of Theoretical Physics, 2019, 58, 4249-4257.	0.5	3
71	Program Obfuscator for Privacy-Carrying Unidirectional One-hop Re-encryption. Lecture Notes in Computer Science, 2015, , 133-142.	1.0	3
72	Efficient signcryption in the standard model. Concurrency Computation Practice and Experience, 2012, 24, 1977-1989.	1.4	2

#	ARTICLE	IF	CITATIONS
73	Key continual-leakage resilient broadcast cryptosystem from dual system in broadcast networks. <i>Frontiers of Computer Science</i> , 2014, 8, 456-468.	1.6	2
74	Unbounded anonymous hierarchical IBE with continual-key-leakage tolerance. <i>Security and Communication Networks</i> , 2014, 7, 1974-1987.	1.0	2
75	Insecurity of an Efficient Identity-Based Proxy Signature in the Standard Model. <i>Computer Journal</i> , 2015, 58, 2507-2508.	1.5	2
76	Strongly average-case secure obfuscation: achieving input privacy and circuit obscurity. <i>Security and Communication Networks</i> , 2016, 9, 1737-1747.	1.0	2
77	Leakage-Resilient Password-Based Authenticated Key Exchange. <i>Lecture Notes in Computer Science</i> , 2017, , 285-296.	1.0	2
78	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> , 2012, E95-A, 259-262.	0.2	2
79	Secure two-party integer comparison protocol without any third party. <i>Quantum Information Processing</i> , 2021, 20, 1.	1.0	2
80	SEPSI: A Secure and Efficient Privacy-Preserving Set Intersection with Identity Authentication in IoT. <i>Mathematics</i> , 2022, 10, 2120.	1.1	2
81	PRIVACY-PRESERVING OLAP FOR ACCURATE ANSWER. <i>Journal of Circuits, Systems and Computers</i> , 2012, 21, 1250009.	1.0	1
82	Analysis and Improvement of a Secret Broadcast with Binding Encryption in Broadcasting Networks. <i>IEICE Transactions on Information and Systems</i> , 2012, E95-D, 686-689.	0.4	1
83	Anonymous encryption with partial-order subset delegation and its application in privacy email systems. <i>IET Information Security</i> , 2014, 8, 240-249.	1.1	1
84	Updatable Lossy Trapdoor Functions Under Consecutive Leakage. <i>Computer Journal</i> , 2020, 63, 648-656.	1.5	1
85	PP-VCA: A Privacy-Preserving and Verifiable Combinatorial Auction Mechanism. <i>Wireless Communications and Mobile Computing</i> , 2020, 2020, 1-11.	0.8	1
86	A Fair $(t, \hat{n})$ -Threshold Secret Sharing Scheme with Efficient Cheater Identifying. <i>IFIP Advances in Information and Communication Technology</i> , 2019, , 122-132.	0.5	1
87	An Efficient Leakage-Resilient Authenticated Group Key Exchange Protocol. <i>Lecture Notes in Computer Science</i> , 2019, , 665-674.	1.0	1
88	Revisits and Transformations Among Functional Encryption Systems. <i>IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)</i> , 2014, 31, 103-114.	2.1	0
89	Fully secure constructions of spatial encryption with vector privacy. <i>International Journal of Communication Systems</i> , 2014, 27, 4307-4327.	1.6	0
90	Generic Constructions and Transformations of Decryption Consistent Encryption. <i>IETE Journal of Research</i> , 2014, 60, 218-228.	1.8	0

#	ARTICLE	IF	CITATIONS
91	Continuous Leakage-Amplified Public-Key Encryption With CCA Security. Computer Journal, 0, , .	1.5	0
92	A Fair and Efficient Secret Sharing Scheme Based on Cloud Assisting. Lecture Notes in Computer Science, 2019, , 348-360.	1.0	0
93	Identity-Based Encryption With Continuous Leakage-Resilient CCA Security From Static Complexity Assumption. Computer Journal, 2023, 66, 924-940.	1.5	0
94	A Gini Coefficient Measurement Method of Income Distribution Gap Based on Privacy-preservation. , 2021, , .		0
95	A Distributed and Privacy-Preserving Random Forest Evaluation Scheme with Fine Grained Access Control. Symmetry, 2022, 14, 415.	1.1	0