Mingwu Zhang

List of Publications by Year in Descending Order

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	Privacy-Enhanced Mean-Variance Scheme Against Malicious Signature Attacks in Smart Grids. *Communications in Computer and Information Science*, **2022**, 145-158	0.3	1
91	A Distributed and Privacy-Preserving Random Forest Evaluation Scheme with Fine Grained Access Control. *Symmetry*, **2022**, 14, 415	2.7	
90	Measurement-device-independent quantum secure multiparty summation. *Quantum Information Processing*, **2022**, 21, 1	1.6	1
89	TPM-Based Conditional Privacy-Preserving Authentication Protocol in VANETs. *Symmetry*, **2022**, 14, 1123	2.7	0
88	Secure two-party integer comparison protocol without any third party. *Quantum Information Processing*, **2021**, 20, 1	1.6	
87	Secure and Efficient Certificate-Based Proxy Signature Schemes for Industrial Internet of Things. *IEEE Systems Journal*, **2021**, 1-12	4.3	2
86	Continuous leakage-resilient certificate-based signcryption scheme and application in cloud computing. *Theoretical Computer Science*, **2021**, 860, 1-22	1.1	3
85	SE-PPFM: A Searchable Encryption Scheme Supporting Privacy-Preserving Fuzzy Multikeyword in Cloud Systems. *IEEE Systems Journal*, **2021**, 15, 2980-2988	4.3	24
84	PPO-DFK: A Privacy-Preserving Optimization of Distributed Fractional Knapsack With Application in Secure Footballer Configurations. *IEEE Systems Journal*, **2021**, 15, 759-770	4.3	11
83	A cloud-aided privacy-preserving multi-dimensional data comparison protocol. *Information Sciences*, **2021**, 545, 739-752	7.7	22
82	PP-OCQ: A distributed privacy-preserving optimal closeness query scheme for social networks. *Computer Standards and Interfaces*, **2021**, 74, 103484	3.5	2
81	Novel Public-Key Encryption with Continuous Leakage Amplification. *Computer Journal*, **2021**, 64, 1163-1177	1.3	3
80	PPDDS: A Privacy-Preserving Disease Diagnosis Scheme Based on the Secure Mahalanobis Distance Evaluation Model. *IEEE Systems Journal*, **2021**, 1-11	4.3	4
79	. *IEEE Access*, **2021**, 9, 70616-70627	3.5	1
78	Improved Secure Transaction Scheme With Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. *IEEE Systems Journal*, **2021**, 1-9	4.3	5
77	Verifiable Quantum Key Exchange with Authentication. *International Journal of Theoretical Physics*, **2021**, 60, 227-242	1.1	4
76	Anonymous quantum voting protocol based on Chinese remainder theorem. *European Physical Journal D*, **2021**, 75, 1	1.3	1

75	A Privacy-Preserving Optimization of Neighborhood-Based Recommendation for Medical-Aided Diagnosis and Treatment. *IEEE Internet of Things Journal*, **2021**, 8, 10830-10842	10.7	21
74	Quantum private set intersection cardinality based on bloom filter. *Scientific Reports*, **2021**, 11, 17332	4.9	2
73	Privacy-Preserving Federated Learning in Medical Diagnosis with Homomorphic Re-Encryption. *Computer Standards and Interfaces*, **2021**, 103583	3.5	4
72	Efficient Obfuscation for Encrypted Identity-Based Signatures in Wireless Body Area Networks. *IEEE Systems Journal*, **2020**, 14, 5320-5328	4.3	3
71	Quantum Secure Multi-party Private Set Intersection Cardinality. *International Journal of Theoretical Physics*, **2020**, 59, 1992-2007	1.1	5
70	A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme. *IEEE Internet of Things Journal*, **2020**, 7, 3083-3093	10.7	14
69	An efficient aggregation scheme resisting on malicious data mining attacks for smart grid. *Information Sciences*, **2020**, 526, 289-300	7.7	26
68	A provable-secure and practical two-party distributed signing protocol for SM2 signature algorithm. *Frontiers of Computer Science*, **2020**, 14, 1	2.2	6
67	Updatable Lossy Trapdoor Functions Under Consecutive Leakage. *Computer Journal*, **2020**, 63, 648-656	1.3	1
66	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. *IEEE Internet of Things Journal*, **2020**, 7, 10660-10672	10.7	58
65	PP-VCA: A Privacy-Preserving and Verifiable Combinatorial Auction Mechanism. *Wireless Communications and Mobile Computing*, **2020**, 2020, 1-11	1.9	1
64	A Secure Clinical Diagnosis With Privacy-Preserving Multiclass Support Vector Machine in Clouds. *IEEE Systems Journal*, **2020**, 1-12	4.3	14
63	A Novel Privacy-Preserving Authentication Scheme for V2G Networks. *IEEE Systems Journal*, **2020**, 14, 1963-1971	4.3	7
62	Cryptanalysis and Improvement of Quantum Sealed-Bid Auction. *International Journal of Theoretical Physics*, **2020**, 59, 1917-1926	1.1	6
61	. *IEEE Access*, **2019**, 7, 72105-72112	3.5	7
60	An efficient and adaptive data-hiding scheme based on secure random matrix. *PLoS ONE*, **2019**, 14, e0223892	3.7	5
59	Privacy-preserving Quantum Sealed-bid Auction Based on Grover's Search Algorithm. *Scientific Reports*, **2019**, 9, 7626	4.9	12
58	. *IEEE Systems Journal*, **2019**, 13, 1478-1486	4.3	26

57	A robust, distributed, and privacy-preserving aggregation scheme for smart grid communications **2019**, 42, 54-65		2
56	Strong Privacy-preserving Two-party Scalar Product Quantum Protocol. *International Journal of Theoretical Physics*, **2019**, 58, 4249-4257	1.1	1
55	A Fair (t, n)-Threshold Secret Sharing Scheme with Efficient Cheater Identifying. *IFIP Advances in Information and Communication Technology*, **2019**, 122-132	0.5	
54	A Fair and Efficient Secret Sharing Scheme Based on Cloud Assisting. *Lecture Notes in Computer Science*, **2019**, 348-360	0.9	
53	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	
52	An Efficient Leakage-Resilient Authenticated Group Key Exchange Protocol. *Lecture Notes in Computer Science*, **2019**, 665-674	0.9	1
51	Accountable mobile E-commerce scheme in intelligent cloud system transactions. *Journal of Ambient Intelligence and Humanized Computing*, **2018**, 9, 1889-1899	3.7	26
50	An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection. *Computer Journal*, **2018**, 61, 526-538	1.3	19
49	After-the-Fact Leakage-Resilient Identity-Based Authenticated Key Exchange. *IEEE Systems Journal*, **2018**, 12, 2017-2026	4.3	19
48	On the Soundness and Security of Privacy-Preserving SVM for Outsourcing Data Classification. *IEEE Transactions on Dependable and Secure Computing*, **2018**, 15, 906-912	3.9	42
47	Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation. *Science China Information Sciences*, **2018**, 61, 1	3.4	29
46	Tolerating Sensitive-Leakage With Larger Plaintext-Space and Higher Leakage-Rate in Privacy-Aware Internet-of-Things. *IEEE Access*, **2018**, 6, 33859-33870	3.5	6
45	. *IEEE Access*, **2018**, 6, 43936-43945	3.5	3
44	Secure and Membership-Based Data Sharing Scheme in V2G Networks. *IEEE Access*, **2018**, 6, 58450-58460	3.5	2
43	Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. *IEEE Systems Journal*, **2017**, 11, 1018-1026	4.3	12
42	Efficient Privacy-Preserving Cube-Data Aggregation Scheme for Smart Grids. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 1369-1381	8	75
41	Leakage-Resilient Password-Based Authenticated Key Exchange. *Lecture Notes in Computer Science*, **2017**, 285-296	0.9	2
40	Obfuscating Re-encryption Algorithm With Flexible and Controllable Multi-Hop on Untrusted Outsourcing Server. *IEEE Access*, **2017**, 5, 26419-26434	3.5	7

39	Provably Leakage-Resilient Password-Based Authenticated Key Exchange in the Standard Model. *IEEE Access*, **2017**, 5, 26832-26841	3.5	9
38	Continuous Leakage Resilient Lossy Trapdoor Functions. *Information (Switzerland)*, **2017**, 8, 38	2.6	2
37	Privacy-friendly weighted-reputation aggregation protocols against malicious adversaries in cloud services. *International Journal of Communication Systems*, **2016**, 29, 1863-1872	1.7	5
36	Realizing secret sharing with general access structure. *Information Sciences*, **2016**, 367-368, 209-220	7.7	15
35	Token-Leakage Tolerant and Vector Obfuscated IPE and Application in Privacy-Preserving Two-Party Point/Polynomial Evaluations. *Computer Journal*, **2016**, 59, 493-507	1.3	4
34	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	1
33	Strongly average-case secure obfuscation: achieving input privacy and circuit obscurity. *Security and Communication Networks*, **2016**, 9, 1737-1747	1.9	2
32	Functional Encryption Resilient to Hard-to-Invert Leakage. *Computer Journal*, **2015**, 58, 735-749	1.3	6
31	Public Key Encryption with Delegated Equality Test in a Multi-User Setting. *Computer Journal*, **2015**, 58, 986-1002	1.3	64
30	Insecurity of an Efficient Identity-Based Proxy Signature in the Standard Model. *Computer Journal*, **2015**, 58, 2507-2508	1.3	2
29	Security analysis of a homomorphic signature scheme for network coding. *Security and Communication Networks*, **2015**, 8, 4053-4060	1.9	11
28	Efficient Public Key Encryption With Equality Test Supporting Flexible Authorization. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 458-470	8	108
27	Program Obfuscator for Privacy-Carrying Unidirectional One-hop Re-encryption. *Lecture Notes in Computer Science*, **2015**, 133-142	0.9	3
26	Generic Constructions and Transformations of Decryption Consistent Encryption. *IETE Journal of Research*, **2014**, 60, 218-228	0.9	
25	LR-FEAD: leakage-tolerating and attribute-hiding functional encryption mechanism with delegation in affine subspaces. *Journal of Supercomputing*, **2014**, 70, 1405-1432	2.5	3
24	Key continual-leakage resilient broadcast cryptosystem from dual system in broadcast networks. *Frontiers of Computer Science*, **2014**, 8, 456-468	2.2	2
23	Anonymous encryption with partial-order subset delegation and its application in privacy email systems. *IET Information Security*, **2014**, 8, 240-249	1.4	1
22	Anonymous spatial encryption under affine space delegation functionality with full security. *Information Sciences*, **2014**, 277, 715-730	7.7	6

21	Unbounded anonymous hierarchical IBE with continual-key-leakage tolerance. *Security and Communication Networks*, **2014**, 7, 1974-1987	1.9	0
20	Revisits and Transformations Among Functional Encryption Systems. *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)*, **2014**, 31, 103-114	1.5	
19	PPGJ: A privacy-preserving general join for outsourced encrypted database. *Security and Communication Networks*, **2014**, 7, 1232-1244	1.9	1
18	An efficient fair UC-secure protocol for two-party computation. *Security and Communication Networks*, **2014**, 7, 1253-1263	1.9	3
17	Fully secure constructions of spatial encryption with vector privacy. *International Journal of Communication Systems*, **2014**, 27, 4307-4327	1.7	
16	Identity-based partially blind signature in the standard model for electronic cash. *Mathematical and Computer Modelling*, **2013**, 58, 196-203		13
15	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	4.3	23
14	Bounded Leakage-Resilient Functional Encryption with Hidden Vector Predicate. *Computer Journal*, **2013**, 56, 464-477	1.3	24
13	Efficient and adaptively secure broadcast encryption systems. *Security and Communication Networks*, **2013**, 6, 1044-1052	1.9	8
12	An ID-based cryptographic mechanisms based on GDLP and IFP. *Information Processing Letters*, **2012**, 112, 753-758	0.8	27
11	Reconciling and improving of multi-receiver signcryption protocols with threshold decryption. *Security and Communication Networks*, **2012**, 5, 1430-1440	1.9	4
10	Efficient signcryption in the standard model. *Concurrency Computation Practice and Experience*, **2012**, 24, 1977-1989	1.4	1
9	PRIVACY-PRESERVING OLAP FOR ACCURATE ANSWER. *Journal of Circuits, Systems and Computers*, **2012**, 21, 1250009	0.9	1
8	Analysis and Improvement of a Secret Broadcast with Binding Encryption in Broadcasting Networks. *IEICE Transactions on Information and Systems*, **2012**, E95-D, 686-689	0.6	1
7	Cryptanalysis of Strong Designated Verifier Signature Scheme with Non-delegatability and Non-transferability. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2012**, E95-A, 259-262	0.4	1
6	LR-UESDE: A Continual-Leakage Resilient Encryption with Unbounded Extensible Set Delegation. *Lecture Notes in Computer Science*, **2012**, 125-142	0.9	4
5	Group-oriented setting□ multisigncryption scheme with threshold designcryption. *Information Sciences*, **2011**, 181, 4041-4050	7.7	5
4	GeoEnc: Geometric Area Based Keys and Policies in Functional Encryption Systems. *Lecture Notes in Computer Science*, **2011**, 241-258	0.9	3

3	Anonymous Encryption with Partial-Order Subset Delegation Functionality. *Lecture Notes in Computer Science*, **2011**, 154-169	0.9	4
2	Efficient Secret Authenticatable Anonymous Signcryption Scheme with Identity Privacy. *Lecture Notes in Computer Science*, **2008**, 126-137	0.9	11
1	Efficient Identity-Based Signcryption Scheme for Multiple Receivers. *Lecture Notes in Computer Science*, **2007**, 13-21	0.9	28