Qiuliang Xu

List of Publications by Year in descending order

68 papers	379 citations	1040056 9 h-index	888059 17 g-index
69 all docs	69 docs citations	69 times ranked	307 citing authors

#	Article	IF	Citations
1	Forward Private Searchable Symmetric Encryption with Optimized I/O Efficiency. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 912-927.	5.4	79
2	Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications. Lecture Notes in Computer Science, 2019, , 147-175.	1.3	60
3	Attribute-based re-encryption scheme in the standard model. Wuhan University Journal of Natural Sciences, 2008, 13, 621-625.	0.4	25
4	A Provably Secure Two-Party Attribute-Based Key Agreement Protocol. , 2009, , .		16
5	Social rational secure multiâ€party computation. Concurrency Computation Practice and Experience, 2014, 26, 1067-1083.	2.2	15
6	Certificateless Proxy Blind Signature Scheme from Bilinear Pairings. , 2009, , .		14
7	A Two-party certificateless authenticated key agreement protocol without pairing. , 2009, , .		14
8	Fair Secure Computation with Reputation Assumptions in the Mobile Social Networks. Mobile Information Systems, 2015, 2015, 1-8.	0.6	12
9	Multi-user searchable encryption with a designated server. Annales Des Telecommunications/Annals of Telecommunications, 2017, 72, 617-629.	2.5	12
10	A brief survey on secure multi-party computing in the presence of rational parties. Journal of Ambient Intelligence and Humanized Computing, 2015, 6, 807-824.	4.9	11
11	Efficient and secure outsourced approximate pattern matching protocol. Soft Computing, 2018, 22, 1175-1187.	3.6	10
12	Rational computing protocol based on fuzzy theory. Soft Computing, 2016, 20, 429-438.	3.6	9
13	An ORAM-based privacy preserving data sharing scheme for cloud storage. Journal of Information Security and Applications, 2018, 39, 1-9.	2.5	9
14	Cut-and-Choose Bilateral Oblivious Transfer and Its Application. , 2015, , .		8
15	New rational parties relying on reputation. Security and Communication Networks, 2014, 7, 1128-1137.	1.5	7
16	Fair twoâ€party computation with rational parties holding private types. Security and Communication Networks, 2015, 8, 284-297.	1.5	6
17	Fast Cut-and-Choose Bilateral Oblivious Transfer for Malicious Adversaries. , 2016, , .		6
18	Secure and efficient two-party certificateless authenticated key agreement protocol. , 2009, , .		5

#	Article	IF	Citations
19	Constructing Secure Two-Party Authenticated Key Agreement Protocol Based on Certificateless Public Key Encryption Scheme. , 2009, , .		4
20	A Secure Threshold Signature Scheme from Lattices. , 2013, , .		4
21	Public-key encryption for protecting data in cloud system with intelligent agents against side-channel attacks. Soft Computing, 2016, 20, 4919-4932.	3.6	4
22	Secure and Efficient Two-Party Authenticated Key Agreement Protocol from Certificateless Public Key Encryption Scheme. , 2009, , .		3
23	Key Replicating Attack on Certificateless Authenticated Key Agreement Protocol. , 2009, , .		3
24	Identity-based broadcast encryption with recipient privacy. , 2010, , .		3
25	A Provably-Secure and Efficient Verifier-Based Anonymous Password-Authenticated Key Exchange Protocol. , 2016, , .		3
26	Research on the Encrypted Data Access Control of Multi-purpose Asynchronous WSN. , 2008, , .		2
27	Identity Based Authenticated Key Agreement for Tree-Based Group. , 2009, , .		2
28	A Strong Designated-verifier Proxy Signature Scheme. , 2009, , .		2
29	On the Security of Certificateless Authenticated Key Agreement Protocol (CL-AK) for Grid Computing. , 2009, , .		2
30	Improved Impossible Differential Cryptanalysis of SMS4. , 2012, , .		2
31	Publicâ€key encryption with keyword search secure against continual memory attacks. Security and Communication Networks, 2016, 9, 1613-1629.	1.5	2
32	An Improvement to a Multi-Client Searchable Encryption Scheme for Boolean Queries. Journal of Medical Systems, 2016, 40, 255.	3.6	2
33	An Efficient Outsourced Oblivious Transfer Extension Protocol and Its Applications. Security and Communication Networks, 2020, 2020, 1-12.	1.5	2
34	Postquantum Cut-and-Choose Oblivious Transfer Protocol Based on LWE. Security and Communication Networks, 2021, 2021, 1-15.	1.5	2
35	Efficient Role Hierarchy Management for T-RBAC Model. , 2006, , .		1
36	Forward-secure digital signature scheme with tamper evidence. Wuhan University Journal of Natural Sciences, 2008, 13, 582-586.	0.4	1

#	Article	IF	Citations
37	Secure Homomorphic Aggregation Algorithm of Mixed Operations in Wireless Sensor Networks. , 2009, , .		1
38	A Secure ID-Based Explicit Authenticated Key Agreement Protocol without Key Escrow. , 2009, , .		1
39	Two-Party Authenticated Key Agreement Protocol from Certificateless Public Key Encryption Scheme. , 2009, , .		1
40	A secure two-party key agreement protocol with key escrow and perfect forward secrecy. , 2009, , .		1
41	An Improved Tripartite Authenticated Key Agreement Protocol from Pairings. , 2010, , .		1
42	Provably secure identity-based key agreement protocols under simple assumption. , 2010, , .		1
43	An identity-based group-oriented threshold encryption scheme. , 2011, , .		1
44	Attribute-Based Authenticated Key Exchange Protocol with General Relations. , 2011, , .		1
45	A new non-interactive deniable authentication protocol based on generalized ElGamal signature scheme. , 2011, , .		1
46	An efficient and secure one-round authenticated key agreement protocol without pairings. , 2011, , .		1
47	A Provably Secure Identity-Based Key Agreement Protocol from Key Encapsulation Scheme. , 2012, , .		1
48	A Simple and Effective Scheme of Ciphertext-Policy ABE. , 2012, , .		1
49	The Electronic Voting in the Presence of Rational Voters. , 2015, , .		1
50	Fast Twoâ€Output Secure Computation with Optimal Error Probability. Chinese Journal of Electronics, 2017, 26, 933-941.	1.5	1
51	Cut-and-choose bilateral oblivious transfer protocol based on DDH assumption. Journal of Ambient Intelligence and Humanized Computing, 2018, , 1.	4.9	1
52	Several Oblivious Transfer Variants in Cut-and-Choose Scenario. International Journal of Information Security and Privacy, 2015, 9, 1-12.	0.8	1
53	Searchable Symmetric Encryption with Tunable Leakage Using Multiple Servers. Lecture Notes in Computer Science, 2020, , 157-177.	1.3	1
54	Privacy-preserving trust negotiation with hidden credentials and hidden policies in a multi-party environment. Wuhan University Journal of Natural Sciences, 2008, 13, 553-556.	0.4	0

#	Article	IF	Citations
55	Perfect Forward Secure Two-Party Key Agreement Protocol with Key Escrow. , 2009, , .		0
56	An Enhanced Two-Party Key Agreement Protocol in the Key Escrow Mode. , 2009, , .		0
57	A Fully Anonymous Identity-Based Signcryption Scheme in the Standard Model. , 2010, , .		0
58	Fairness with Semi-rational Players in Standard Communication Networks. , 2011, , .		0
59	2-out-of-2 Rational Secret Sharing in Extensive Form. , 2011, , .		0
60	A Permanent Secure QKD Protocol Realized with Asymmetric Key Authentication. , 2012, , .		0
61	Multi-party Computation with Social Rational Parties. , 2012, , .		0
62	Fair Computation with Tit-for-Tat Strategy. , 2013, , .		0
63	Identity-Based Authenticate Key Exchange Protocol from Lattice. , 2013, , .		0
64	Achieving fairness by sequential equilibrium in rational twoâ€party computation under incomplete information. Security and Communication Networks, 2015, 8, 3690-3700.	1.5	0
65	Longest Common Sub-sequence Computation and Retrieve for Encrypted Character Strings. , 2016, , .		0
66	An Efficient CPA-Secure Encryption Scheme with Equality Test. , 2017, , .		0
67	Post-Quantum Universal Composable OT Based on Key Exchange. IEEE Access, 2020, 8, 148445-148459.	4.2	0
68	EPPSA: Efficient Privacy-Preserving Statistical Aggregation Scheme for Edge Computing-Enhanced Wireless Sensor Networks. Security and Communication Networks, 2022, 2022, 1-12.	1.5	0