Jiang Zhang

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4687430/publications.pdf

Version: 2024-02-01

32	486	933447 10	713466 21
papers	citations	h-index	g-index

34	34	34	373
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Non-Malleable Functions and their Applications. Journal of Cryptology, 2022, 35, 1.	2.8	2
2	An Efficient NIZK Scheme for Privacy-Preserving Transactions Over Account-Model Blockchain. IEEE Transactions on Dependable and Secure Computing, 2021, 18, 641-651.	5.4	48
3	Smoothing Out Binary Linear Codes and Worst-Case Sub-exponential Hardness for LPN. Lecture Notes in Computer Science, 2021, , 473-501.	1.3	3
4	Lattice-Based Cryptosystems. , 2020, , .		3
5	Digital Signatures. , 2020, , 145-174.		0
6	Identity-Based Encryption. , 2020, , 51-76.		0
7	Public-key Encryption. , 2020, , 23-49.		0
8	A Practical NIZK Argument for Confidential Transactions over Account-Model Blockchain. Lecture Notes in Computer Science, 2020, , 234-253.	1.3	2
9	Key Exchanges. , 2020, , 93-144.		0
10	Attribute-Based Encryption. , 2020, , 77-91.		0
11	Lattices. , 2020, , 7-21.		0
12	Collision Resistant Hashing from Sub-exponential Learning Parity with Noise. Lecture Notes in Computer Science, 2019, , 3-24.	1.3	5
13	On the Hardness of Learning Parity with Noise over Rings. Lecture Notes in Computer Science, 2018, , 94-108.	1.3	0
14	Anonymous Password Authenticated Key Exchange Protocol in the Standard Model. Wireless Personal Communications, 2017, 96, 1451-1474.	2.7	5
15	Universally composable anonymous password authenticated key exchange. Science China Information Sciences, 2017, 60, 1.	4.3	5
16	Cryptography with Auxiliary Input and Trapdoor from Constant-Noise LPN. Lecture Notes in Computer Science, 2016, , 214-243.	1.3	31
17	Programmable Hash Functions from Lattices: Short Signatures and IBEs with Small Key Sizes. Lecture Notes in Computer Science, 2016, , 303-332.	1.3	44
18	Generic constructions of integrated PKE and PEKS. Designs, Codes, and Cryptography, 2016, 78, 493-526.	1.6	23

#	Article	IF	Citations
19	Non-Malleable Functions and Their Applications. Lecture Notes in Computer Science, 2016, , 386-416.	1.3	12
20	Secure and efficient dataâ€sharing in clouds. Concurrency Computation Practice and Experience, 2015, 27, 2125-2143.	2.2	16
21	Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks. Lecture Notes in Computer Science, 2015, , 140-153.	1.3	9
22	Simpler Efficient Group Signatures from Lattices. Lecture Notes in Computer Science, 2015, , 401-426.	1.3	67
23	Authenticated Key Exchange from Ideal Lattices. Lecture Notes in Computer Science, 2015, , 719-751.	1.3	92
24	PRE: Stronger security notions and efficient construction with non-interactive opening. Theoretical Computer Science, 2014, 542, 1-16.	0.9	10
25	Proxy Re-encryption with Unforgeable Re-encryption Keys. Lecture Notes in Computer Science, 2014, , 20-33.	1.3	8
26	Black-Box Separations for One-More (Static) CDH and Its Generalization. Lecture Notes in Computer Science, 2014, , 366-385.	1.3	10
27	Secure and Efficient Data-Sharing in Clouds. , 2013, , .		0
28	Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme. IEEE Transactions on Parallel and Distributed Systems, 2013, 24, 2319-2321.	5.6	26
29	Towards a Secure Certificateless Proxy Re-Encryption Scheme. Lecture Notes in Computer Science, 2013, , 330-346.	1.3	10
30	Ciphertext policy attribute-based encryption from lattices. , 2012, , .		31
31	A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings. Lecture Notes in Computer Science, 2012, , 324-340.	1.3	19
32	A Generic Construction from Selective-IBE to Public-Key Encryption with Non-interactive Opening. Lecture Notes in Computer Science, 2012, , 195-209.	1.3	3