Mengce Zheng

List of Publications by Year
in descending order

17 papers	**57** citations	1684188 **5** h-index	1720034 **7** g-index
18 all docs	**18** docs citations	**18** times ranked	**35** citing authors

#	Article	IF	Citations
1	A practical quantum designated verifier signature scheme for E-voting applications. Quantum Information Processing, 2021, 20, 1.	2.2	15
2	Cryptanalysis of Prime Power RSA with two private exponents. Science China Information Sciences, 2015, 58, 1-8.	4.3	7
3	Cryptanalysis of the RSA variant based on cubic Pell equation. Theoretical Computer Science, 2021, 889, 135-144.	0.9	6
4	Cryptanalysis of RSA Variants withÂModified Euler Quotient. Lecture Notes in Computer Science, 2018, , 266-281.	1.3	5
5	Bibliometrics of Machine Learning Research Using Homomorphic Encryption. Mathematics, 2021, 9, 2792.	2.2	5
6	Generalized cryptanalysis of RSA with small public exponent. Science China Information Sciences, 2016, 59, 1.	4.3	4
7	An improved QKD protocol without public announcement basis using periodically derived basis. Quantum Information Processing, 2021, 20, 1.	2.2	4
8	Lattice-Based Cryptanalysis of RSA with Implicitly Related Keys. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2020, E103.A, 959-968.	0.3	4
9	Implicit Related-Key Factorization Problem on the RSA Cryptosystem. Lecture Notes in Computer Science, 2019, , 525-537.	1.3	2
10	Attacking FPGA-based Dual Complementary AES Implementation Using HD and SD Models. , 2020, , .		2
11	Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. Lecture Notes in Computer Science, 2017, , 324-342.	1.3	1
12	Symmetric Lattice-Based PAKE from Approximate Smooth Projective Hash Function and Reconciliation Mechanism. Communications in Computer and Information Science, 2019, , 95-106.	0.5	1
13	Revisiting the Polynomial-Time Equivalence of Computing the CRT-RSA Secret Key and Factoring. Mathematics, 2022, 10, 2238.	2.2	1
14	Generic Generating Functions for the Counting Functions of Quadratic Functions with Prescribed Walsh Spectrum. , 2018, , .		0
15	Post-Quantum Pseudorandom Functions from Mersenne Primes. Communications in Computer and Information Science, 2019, , 128-142.	0.5	0
16	Implicit-Key Attack on the RSA Cryptosystem. Lecture Notes in Computer Science, 2019, , 354-362.	1.3	0
17	A General Construction for Password-Based Authenticated Key Exchange from Witness PRFs. Communications in Computer and Information Science, 2019, , 253-267.	0.5	0