Muhammad Rezal Bin Kamel Ariffin

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/171/publications.pdf

Version: 2024-02-01

25 papers	96 citations	1478505 6 h-index	1474206 9 g-index
25 all docs	25 docs citations	25 times ranked	40 citing authors

#	Article	IF	Citations
1	Exponential increment of RSA attack range via lattice based cryptanalysis. Multimedia Tools and Applications, 2022, 81, 36607-36622.	3.9	3
2	Increment of insecure RSA private exponent bound through perfect square RSA diophantine parameters cryptanalysis. Computer Standards and Interfaces, 2022, 80, 103584.	5.4	3
3	Security Issues of Novel RSA Variant. IEEE Access, 2022, 10, 53788-53796.	4.2	6
4	New Jochemszâ€“May Cryptanalytic Bound for RSA System Utilizing Common Modulus N = p2q. Mathematics, 2021, 9, 340.	2.2	2
5	Analytical cryptanalysis upon N = p2q utilizing Jochemsz-May strategy. PLoS ONE, 2021, 16, e0248888.	2.5	2
6	Determination of a Good Indicator for Estimated Prime Factor and Its Modification in Fermatâ€™s Factoring Algorithm. Symmetry, 2021, 13, 735.	2.2	6
7	URASP: An ultralightweight RFID authentication scheme using permutation operation. Peer-to-Peer Networking and Applications, 2021, 14, 3737-3757.	3.9	11
8	Classical Attacks on a Variant of the RSA Cryptosystem. Lecture Notes in Computer Science, 2021, , 151-167.	1.3	6
9	A Security-Mediated Encryption Scheme Based on ElGamal Variant. Mathematics, 2021, 9, 2642.	2.2	0
10	Mathematical epidemiologic and simulation modelling of first wave COVID-19 in Malaysia. Scientific Reports, 2021, 11, 20739.	3.3	6
11	Factoring the Modulus of Type N = p2q by Finding Small Solutions of the Equation er â^' (Ns + t) = Î±p2 + Î²q2. Mathematics, 2021, 9, 2931.	2.2	0
12	Partial Key Attack Given MSBs of CRT-RSA Private Keys. Mathematics, 2020, 8, 2188.	2.2	3
13	A New LSB Attack on Special-Structured RSA Primes. Symmetry, 2020, 12, 838.	2.2	3
14	On the Improvement Attack Upon Some Variants of RSA Cryptosystem via the Continued Fractions Method. IEEE Access, 2020, 8, 80997-81006.	4.2	8
15	Attacking RSA Using an Arbitrary Parameter. Lecture Notes in Computer Science, 2020, , 382-399.	1.3	0
16	(In)Security of the AAÎ² Cryptosystem for Transmitting Large Data. , 2019, , .		1
17	Commuting Graphs, C(G, X) in Symmetric Groups Sym(n) and Its Connectivity. Symmetry, 2019, 11, 1178.	2.2	2
18	New cryptanalytic results upon prime power moduli N = prq. AIP Conference Proceedings, 2019, , .	0.4	0

#	Article	IF	Citations
19	New Cryptanalytic Attack on RSA Modulus N=pq Using Small Prime Difference Method. Cryptography, 2019, 3, 2.	2.3	13
20	SPA on Rabin variant with public key $$N=p^2q$$ N = p 2 q. Journal of Cryptographic Engineering, 2016, 6, 339-346.	1.8	0
21	Implicit factorization of unbalanced RSA moduli. Journal of Applied Mathematics and Computing, 2015, 48, 349-363.	2.5	4
22	A novel psychovisual model on an independent video frame for an almost lossless compression. , 2014, , .		0
23	New Attacks on the RSA Cryptosystem. Lecture Notes in Computer Science, 2014, , 178-198.	1.3	15
24	The diophantine equation hard problem (DEHP) as an asymmetric primitive - Is it possible?. , 2013, , .		0
25	ANOTHER PROOF OF WIENER'S SHORT SECRET EXPONENT. Malaysian Journal of Science, 0, 38, 67-73.	0.3	2