Chang-An Zhao

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3253515/publications.pdf

Version: 2024-02-01

26

papers

239

citations

1307594

7

h-index

996975

15

g-index

27

all docs

27

docs citations

27

times ranked

128

citing authors

#	Article	IF	Citations
1	Software Implementation of Optimal Pairings on Elliptic Curves with Odd Prime Embedding Degrees. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022, E105.A, 858-870.	0.3	3
2	Trace representation of the binary pq2-periodic sequences derived from Euler quotients. Cryptography and Communications, 2021, 13, 343-359.	1.4	3
3	Good polynomials for optimal LRC of low locality. Designs, Codes, and Cryptography, 2021, 89, 1639-1660.	1.6	3
4	Fast scalar multiplication of degenerate divisors for hyperelliptic curve cryptosystems. Applied Mathematics and Computation, 2021, 404, 126239.	2.2	0
5	Linear Complexity of a Family of Binary pq 2-Periodic Sequences From Euler Quotients. IEEE Transactions on Information Theory, 2020, 66, 5774-5780.	2.4	5
6	Division polynomialâ€based elliptic curve scalar multiplication revisited. IET Information Security, 2019, 13, 614-617.	1.7	1
7	Linear Complexity and Trace Presentation of Sequences with Period 2P2. , 2018, , .		4
8	A class of three-weight linear codes and their complete weight enumerators. Cryptography and Communications, 2017, 9, 133-149.	1.4	22
9	The weight distributions of two classes of p-ary cyclic codes with few weights. Finite Fields and Their Applications, 2017, 44, 76-91.	1.0	50
10	Note on scalar multiplication using division polynomials. IET Information Security, 2017, 11, 195-198.	1.7	7
11	Multi-Point Codes From Generalized Hermitian Curves. IEEE Transactions on Information Theory, 2016, 62, 2726-2736.	2.4	5
12	An Improvement of the Elliptic Net Algorithm. IEEE Transactions on Computers, 2016, 65, 2903-2909.	3.4	3
13	The linear complexity of a class of binary sequences with period $$2p$$ 2 p. Applicable Algebra in Engineering, Communications and Computing, 2015, 26, 475-491.	0.5	7
14	The weight enumerator of the duals of a class of cyclic codes with three zeros. Applicable Algebra in Engineering, Communications and Computing, 2015, 26, 347-367.	0.5	20
15	Erratum Self-pairings on hyperelliptic curves [J. Math. Cryptol. 7 (2013), 31â€"42]. Journal of Mathematical Cryptology, 2014, 8, .	0.7	0
16	Self-pairings on supersingular elliptic curves with embedding degree three. Finite Fields and Their Applications, 2014, 28, 79-93.	1.0	3
17	Self-pairings on hyperelliptic curves. Journal of Mathematical Cryptology, 2013, 7, .	0.7	3
18	Efficient Arithmetic on Elliptic Curves over Fields of Characteristic Three. Lecture Notes in Computer Science, 2013, , 135-148.	1.3	7

#	Article	IF	Citations
19	A progressive interpolation approach for Guruswami-Sudan algorithm. , 2012, , .		0
20	Faster Computation of Self-Pairings. IEEE Transactions on Information Theory, 2012, 58, 3266-3272.	2.4	12
21	Computing bilinear pairings on elliptic curves with automorphisms. Designs, Codes, and Cryptography, 2011, 58, 35-44.	1.6	14
22	Linear complexity of generalized cyclotomic binary sequences of length 2p m. Applicable Algebra in Engineering, Communications and Computing, 2010, 21, 93-108.	0.5	19
23	On the Linear Complexity of Generalized Cyclotomic Binary Sequences with Length 2p2. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 302-308.	0.3	3
24	Research and Development on Efficient Pairing Computations. Ruan Jian Xue Bao/Journal of Software, 2009, 20, 3001-3009.	0.3	4
25	Improved Implementations of Cryptosystems Based on Tate Pairing. Lecture Notes in Computer Science, 2009, , 145-151.	1.3	0
26	A note on the Ate pairing. International Journal of Information Security, 2008, 7, 379-382.	3.4	41