Shuhong Gao

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11174824/publications.pdf

Version: 2024-02-01

39	980	516710	477307
papers	citations	16	29
		h-index	g-index

39	39	39	376
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	An Ultra-Highly Parallel Polynomial Multiplier for the Bootstrapping Algorithm in a Fully Homomorphic Encryption Scheme. Journal of Signal Processing Systems, 2021, 93, 643-656.	2.1	6
2	High-Speed Modular Multiplier for Lattice-Based Cryptosystems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 2927-2931.	3.0	12
3	Counting roots for polynomials modulo prime powers. The Open Book Series, 2019, 2, 191-205.	0.1	2
4	The LaSalle's invariant sets for a class of Lotka-Volterra prey-predator chain systems. Journal of Mathematical Analysis and Applications, 2019, 475, 985-998.	1.0	0
5	Sparse univariate polynomials with many roots over finite fields. Finite Fields and Their Applications, 2017, 46, 235-246.	1.0	5
6	A new framework for computing GrÃ¶bner bases. Mathematics of Computation, 2015, 85, 449-465.	2.1	32
7	Extracting sparse factors from multivariate integral polynomials. Journal of Symbolic Computation, 2013, 52, 3-16.	0.8	5
8	The optimal linear secret sharing scheme for any given access structure. Journal of Systems Science and Complexity, 2013, 26, 634-649.	2.8	8
9	Leakproof secret sharing protocols with applications to group identification scheme. Science China Information Sciences, 2012, 55, 1172-1185.	4.3	4
10	Solving the 100 Swiss Francs Problem. Mathematics in Computer Science, 2011, 5, 195-207.	0.4	3
11	Additive Fast Fourier Transforms Over Finite Fields. IEEE Transactions on Information Theory, 2010, 56, 6265-6272.	2.4	46
12	A new incremental algorithm for computing Groebner bases. , 2010, , .		36
13	Finite field elements of high order arising from modular curves. Designs, Codes, and Cryptography, 2009, 51, 301-314.	1.6	13
14	Short containers in Cayley graphs. Discrete Applied Mathematics, 2009, 157, 1354-1363.	0.9	13
15	On Disjoint Shortest Paths Routing on the Hypercube. Lecture Notes in Computer Science, 2009, , 375-383.	1.3	7
16	Fault Tolerance of Cayley Graphs. Annals of Combinatorics, 2007, 11, 161-171.	0.6	3
17	Deterministic distinct-degree factorization of polynomials over finite fields. Journal of Symbolic Computation, 2004, 38, 1461-1470.	0.8	7
18	Irreducibility of polynomials modulo p via Newton polytopes. Journal of Number Theory, 2003, 101, 32-47.	0.4	19

#	Article	IF	Citations
19	Random Krylov Spaces over Finite Fields. SIAM Journal on Discrete Mathematics, 2003, 16, 276-287.	0.8	30
20	A New Algorithm for Decoding Reed-Solomon Codes. , 2003, , 55-68.		74
21	Finite field multiplier using redundant representation. IEEE Transactions on Computers, 2002, 51, 1306-1316.	3.4	66
22	Factoring multivariate polynomials via partial differential equations. Mathematics of Computation, 2002, 72, 801-823.	2.1	76
23	Hensel lifting and bivariate polynomial factorisation over finite fields. Mathematics of Computation, 2001, 71, 1663-1677.	2.1	21
24	Abelian Groups, Gauss Periods, and Normal Bases. Finite Fields and Their Applications, 2001, 7, 149-164.	1.0	14
25	Absolute Irreducibility of Polynomials via Newton Polytopes. Journal of Algebra, 2001, 237, 501-520.	0.7	62
26	On the Deterministic Complexity of Factoring Polynomials. Journal of Symbolic Computation, 2001, 31, 19-36.	0.8	13
27	Algorithms for Exponentiation in Finite Fields. Journal of Symbolic Computation, 2000, 29, 879-889.	0.8	71
28	Elements of provable high orders in finite fields. Proceedings of the American Mathematical Society, 1999, 127, 1615-1623.	0.8	36
29	From Hall's Matching Theorem to Optimal Routing on Hypercubes. Journal of Combinatorial Theory Series B, 1998, 74, 291-301.	1.0	26
30	Gauss periods: orders and cryptographical applications. Mathematics of Computation, 1998, 67, 343-352.	2.1	37
31	Density of Normal Elements. Finite Fields and Their Applications, 1997, 3, 141-150.	1.0	12
32	Specific irreducible polynomials with linearly independent roots over finite fields. Linear Algebra and Its Applications, 1997, 253, 227-249.	0.9	5
33	Tests and Constructions of Irreducible Polynomials over Finite Fields. , 1997, , 346-361.		19
34	On orders of optimal normal basis generators. Mathematics of Computation, 1995, 64, 1227-1233.	2.1	27
35	Gauss periods and fast exponentiation in finite fields. Lecture Notes in Computer Science, 1995, , 311-322.	1.3	32
36	Constructive problems for irreducible polynomials over finite fields. Lecture Notes in Computer Science, 1994, , 1-23.	1.3	16

#	Article	IF	Citations
37	Normal and Self-Dual Normal Bases from Factorization of $cx^{q + 1} + dx^q - ax - b$. SIAM Journal on Discrete Mathematics, 1994, 7, 499-512.	0.8	10
38	Explicit factorization of $$x^{2^k }$$ + 1 overF p with primep?3 mod 4. Applicable Algebra in Engineering, Communications and Computing, 1993, 4, 89-94.	0.5	34
39	Optimal normal bases. Designs, Codes, and Cryptography, 1992, 2, 315-323.	1.6	78