M Anwar Hasan

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/9145992/publications.pdf

Version: 2024-02-01

33 papers	730 citations	687220 13 h-index	552653 26 g-index
34 all docs	34 docs citations	34 times ranked	383 citing authors

#	Article	IF	Citations
1	A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields. IEEE Transactions on Computers, 2007, 56, 224-233.	2.4	109
2	High-Performance Architecture of Elliptic Curve Scalar Multiplication. IEEE Transactions on Computers, 2008, 57, 1443-1453.	2.4	107
3	Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems. IEEE Transactions on Parallel and Distributed Systems, 2013, 24, 2375-2385.	4.0	76
4	Subquadratic Computational Complexity Schemes for Extended Binary Field Multiplication Using Optimal Normal Bases. IEEE Transactions on Computers, 2007, 56, 1435-1437.	2.4	46
5	Fast Bit Parallel-Shifted Polynomial Basis Multipliers in &lt;formula formulatype="inline"&gt;&lt;tex&gt;$GF(2^{n})$&lt;/tex&gt;&lt;/formula&gt;. IEEE Transactions on Circuits and Systems Part 1: Regular Papers, 2006, 53, 2606-2615.	0.1	44
6	A digital rights management system based on a scalable blockchain. Peer-to-Peer Networking and Applications, 2021, 14, 2665-2680.	2.6	42
7	On Concurrent Detection of Errors in Polynomial Basis Multiplication. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2007, 15, 413-426.	2.1	35
8	Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers. , 2012, , .		34
9	Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae. IEEE Transactions on Computers, 2007, 56, 716-717.	2.4	25
10	Multiway Splitting Method for Toeplitz Matrix Vector Product. IEEE Transactions on Computers, 2013, 62, 1467-1471.	2.4	25
11	Improved Three-Way Split Formulas for Binary Polynomial and Toeplitz Matrix Vector Products. IEEE Transactions on Computers, 2013, 62, 1345-1361.	2.4	23
12	Asymmetric Squaring Formulae. Computer Arithmetic, IEEE Symposium on, 2007, , .	0.0	21
13	On binary signed digit representations of integers. Designs, Codes, and Cryptography, 2006, 42, 43-65.	1.0	16
14	Efficient Subquadratic Space Complexity Binary Polynomial Multipliers Based on Block Recombination. IEEE Transactions on Computers, 2014, 63, 2273-2287.	2.4	16
15	Some new results on binary polynomial multiplication. Journal of Cryptographic Engineering, 2015, 5, 289-303.	1.5	13
16	Low Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation. IEEE Transactions on Computers, 2011, 60, 602-607.	2.4	11
17	Low-Weight Polynomial Form Integers for Efficient Modular Multiplication. IEEE Transactions on Computers, 2007, 56, 44-57.	2.4	9
18	SPA-resistant binary exponentiation with optimal execution time. Journal of Cryptographic Engineering, 2011, 1, 87-99.	1.5	9

#	Article	IF	Citations
19	Toeplitz Matrix Approach for Binary Field Multiplication Using Quadrinomials. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2012, 20, 449-458.	2.1	9
20	Montgomery Reduction Algorithm for Modular Multiplication Using Low-Weight Polynomial Form Integers. Computer Arithmetic, IEEE Symposium on, 2007, , .	0.0	7
21	Efficient Double Bases for Scalar Multiplication. IEEE Transactions on Computers, 2015, 64, 2204-2212.	2.4	7
22	Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms. IEEE Access, 2021, 9, 71295-71317.	2.6	7
23	Algorithm-level error detection for Montgomery ladder-based ECSM. Journal of Cryptographic Engineering, 2011, 1, 57-69.	1.5	6
24	Energy Consumption Analysis of XRP Validator. , 2020, , .		6
25	Sequential multiplier with sub-linear gate complexity. Journal of Cryptographic Engineering, 2012, 2, 91-97.	1.5	5
26	Energy Efficiency Analysis of Elliptic Curve Based Cryptosystems. , 2018, , .		5
27	On Ï„-adic representations of integers. Designs, Codes, and Cryptography, 2007, 45, 271-296.	1.0	4
28	Fault-Based Attack on Montgomeryâ€™s Ladder Algorithm. Journal of Cryptology, 2011, 24, 346-374.	2.1	3
29	Random Digit Representation of Integers. , 2016, , .		3
30	Low complexity parallel multiplier in F(q/sup n/) over F/sub q/. IEEE Transactions on Circuits and Systems Part 1: Regular Papers, 2002, 49, 1009-1013.	0.1	2
31	High performance GHASH and impacts of a class of unconventional bases. Journal of Cryptographic Engineering, 2011, 1, 201-218.	1.5	2
32	Post-Quantum Two-Party Adaptor Signature Based on Coding Theory. Cryptography, 2022, 6, 6.	1.4	2
33	Exp-HE: a family of fast exponentiation algorithms resistant to SPA, fault, and combined attacks. , 2015, , .		1