Dowon Hong

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/2246160/publications.pdf

Version: 2024-02-01

68 papers	650 citations	687363 13 h-index	610901 24 g-index
72 all docs	72 docs citations	72 times ranked	454 citing authors

#	Article	IF	Citations
1	Evaluating differentially private decision tree model over model inversion attack. International Journal of Information Security, 2022, 21, 1-14.	3.4	1
2	Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems. Security and Communication Networks, 2021, 2021, 1-12.	1.5	32
3	Evaluating Differentially Private Generative Adversarial Networks Over Membership Inference Attack. IEEE Access, 2021, 9, 167412-167425.	4.2	3
4	Efficient Bit-Parallel Multiplier for All Trinomials Based on n-Term Karatsuba Algorithm. IEEE Access, 2020, 8, 173491-173507.	4.2	3
5	Space Efficient $GF(2^m)$ Multiplier for Special Pentanomials Based on $n$ -Term Karatsuba Algorithm. IEEE Access, 2020, 8, 27342-27360.	4.2	1
6	An Attack-Based Evaluation Method for Differentially Private Learning Against Model Inversion Attack. IEEE Access, 2019, 7, 124988-124999.	4.2	14
7	Low Space Complexity &lt;inline-formula&gt; &lt;tex-math notation="LaTeX"&gt;$GF(2^m)$ &lt;/tex-math&gt; &lt;/inline-formula&gt; Multiplier for Trinomials Using &lt;inline-formula&gt; &lt;tex-math notation="LaTeX"&gt;$n$ &lt;/tex-math&gt; &lt;/inline-formula&gt;-Term Karatsuba Algorithm. IEEE Access, 2019, 7, 27047-27064.	4.2	5
8	A Symmetric Key Based Deduplicatable Proof of Storage for Encrypted Data in Cloud Storage Environments. Security and Communication Networks, 2018, 2018, 1-16.	1.5	1
9	Subquadratic Space Complexity Multiplier Using Even Type GNB Based on Efficient Toeplitz Matrix-Vector Product. IEEE Transactions on Computers, 2018, 67, 1794-1805.	3.4	0
10	Efficient Three-Way Split Formulas for Binary Polynomial Multiplication and Toeplitz Matrix Vector Product. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 239-248.	0.3	0
11	Efficient multiplier based on hybrid approach for Toeplitz matrixâ€“vector product. Information Processing Letters, 2018, 131, 33-38.	0.6	0
12	New Block Recombination for Subquadratic Space Complexity Polynomial Multiplication Based on Overlap-Free Approach. IEEE Transactions on Computers, 2017, 66, 1396-1406.	3.4	3
13	Efficient Multiplication Based on Dickson Bases over Any Finite Fields. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 2060-2074.	0.3	2
14	Explicit formulae for Mastrovito matrix and its corresponding Toeplitz matrix for all irreducible pentanomials using shifted polynomial basis. The Integration VLSI Journal, 2016, 53, 27-38.	2.1	1
15	Comments on â€œMultiway Splitting Method for Toeplitz Matrix Vector Productâ€• IEEE Transactions on Computers, 2016, 65, 332-333.	3.4	3
16	Symmetric searchable encryption with efficient range query using multi-layered linked chains. Journal of Supercomputing, 2016, 72, 4233-4246.	3.6	10
17	Encrypted Data Deduplication Using Key Issuing Server. Journal of KIISE, 2016, 43, 143-151.	0.1	1
18	Generalization to Any Field of Toeplitz Matrix Vector Product Based on Multi-Way Splitting Method and Its Application. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 378-383.	0.3	3

#	Article	IF	Citations
19	Low Complexity Multiplier Based on Dickson Basis Using Efficient Toeplitz Matrix-Vector Product. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 2283-2290.	0.3	4
20	Comments on â€œOn the Polynomial Multiplication in Chebyshev Formâ€. IEEE Transactions on Computers, 2014, 63, 3162-3163.	3.4	1
21	New efficient bit-parallel polynomial basis multiplier for special pentanomials. The Integration VLSI Journal, 2014, 47, 130-139.	2.1	12
22	Bit-Parallel Cubing Computation over <i>GF</i>(3<i><sup>m</sup></i>) for Irreducible Trinomials. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 347-353.	0.3	1
23	Authenticated Distance Bounding Protocol with Improved FAR: Beyond the Minimal Bound of FAR. IEICE Transactions on Communications, 2014, E97.B, 930-935.	0.7	2
24	Bucket Index Ordering Problem in Range Queries. Lecture Notes in Electrical Engineering, 2014, , 347-355.	0.4	0
25	Privacy-preserving disjunctive normal form operations on distributed sets. Information Sciences, 2013, 231, 113-122.	6.9	17
26	Parallel multiplier for trinomials. Information Processing Letters, 2013, 113, 111-115.	0.6	1
27	Identity-based proxy signature from lattices. Journal of Communications and Networks, 2013, 15, 1-7.	2.6	23
28	Subquadratic Space Complexity Multiplier for &lt;i&gt;GF&lt;/i&gt;(2&lt;sup&gt;n&lt;/sup&gt;) Using Type 4 Gaussian Normal Bases. ETRI Journal, 2013, 35, 523-529.	2.0	7
29	Fast Bit-Parallel Polynomial Basis Multiplier for &lt;i&gt;GF&lt;/i&gt;(2&lt;i&gt;&lt;sup&gt;m&lt;/sup&gt;&lt;/i&gt;) Defined by Pentanomials Using Weakly Dual Basis. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 322-331.	0.3	1
30	A Strong Binding Encryption Scheme from Lattices for Secret Broadcast. IEEE Communications Letters, 2012, 16, 781-784.	4.1	1
31	Signcryption with fast online signing and short signcryptext for secure and private mobile communication. Science China Information Sciences, 2012, 55, 2530-2541.	4.3	7
32	Scalable Privacy-Preserving <i>t</i>-Repetition Protocol with Distributed Medical Data. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95.A, 2451-2460.	0.3	0
33	Pervasive Forensic Analysis Based on Mobile Cloud Computing. , 2011, , .		21
34	Security problem on arbitrated quantum signature schemes. Physical Review A, 2011, 84, .	2.5	81
35	On Fast Private Scalar Product Protocols. Communications in Computer and Information Science, 2011, , 1-10.	0.5	2
36	Privacy Preserving Association Rule Mining Revisited: Privacy Enhancement and Resources Efficiency. IEICE Transactions on Information and Systems, 2010, E93-D, 315-325.	0.7	5

#	Article	IF	Citations
37	Augmented Rotation-Based Transformation for Privacy-Preserving Data Clustering. ETRI Journal, 2010, 32, 351-361.	2.0	8
38	Constructing PEKS schemes secure against keyword guessing attacks is possible?. Computer Communications, 2009, 32, 394-396.	5.1	106
39	Improving Performance in Digital Forensics: A Case Using Pattern Matching Board. , 2009, , .		3
40	Searchable Encryption with Keyword-Recoverability. IEICE Transactions on Information and Systems, 2009, E92-D, 1200-1203.	0.7	3
41	High-speed search using Tarari content processor in digital forensics. Digital Investigation, 2008, 5, S91-S95.	3.2	13
42	Data Randomization for Lightweight Secure Data Aggregation in Sensor Network. Lecture Notes in Computer Science, 2008, , 338-351.	1.3	0
43	Windows Registry and Hiding Suspects' Secret in Registry. , 2008, , .		4
44	Privacy in Location Based Services: Primitives Toward the Solution. , 2008, , .		7
45	A Forensic Investigation for Suspects' Digital Evidences Using Image Categorization. , 2008, , .		1
46	Defense technology of anti forensic. , 2008, , .		0
47	High Speed Search for Large-Scale Digital Forensic Investigation. , 2008, , .		1
48	Suspects' data hiding at remaining registry values of uninstalled programs. , 2008, , .		3
49	Mitigating the ICA Attack against Rotation-Based Transformation for Privacy Preserving Clustering. ETRI Journal, 2008, 30, 868-870.	2.0	5
50	Forensics for Korean Cell Phone. , 2008, , .		1
51	Protection Techniques of Secret Information in Non-tamper Proof Devices of Smart Home Network. Lecture Notes in Computer Science, 2008, , 548-562.	1.3	0
52	A New Anti-Forensic Tool Based on a Simple Data Encryption Scheme. , 2007, , .		1
53	Chosen Message Attack Against Mukherjee-Ganguly-Chaudhuriâ€™s Message Authentication Scheme. Lecture Notes in Computer Science, 2007, , 427-434.	1.3	0
54	Cryptanalysis of Mukherjee-Ganguly-Chaudhuri's Message Authentication Scheme. , 2006, , .		0

#	Article	IF	Citations
55	Efficient Bit-Parallel Multiplier for Irreducible Pentanomials Using a Shifted Polynomial Basis. IEEE Transactions on Computers, 2006, 55, 1211-1215.	3.4	18
56	Efficient Exponentiation in GF(p m) Using the Frobenius Map. Lecture Notes in Computer Science, 2006, , 584-593.	1.3	0
57	A DPA Countermeasure by Randomized Frobenius Decomposition. Lecture Notes in Computer Science, 2006, , 271-282.	1.3	0
58	Padding Oracle Attacks on Multiple Modes of Operation. Lecture Notes in Computer Science, 2005, , 343-351.	1.3	4
59	Low Complexity Bit-Parallel Multiplier for GF(2^m) Defined by All-One Polynomials Using Redundant Representation. IEEE Transactions on Computers, 2005, 54, 1628-1630.	3.4	20
60	An efficient key distribution scheme with self-healing property. IEEE Communications Letters, 2005, 9, 759-761.	4.1	62
61	Validation Testing Tool for Light-Weight Stream Ciphers. The KIPS Transactions PartC, 2005, 12C, 495-502.	0.2	0
62	An Efficient Variant of Self-Healing Group Key Distribution Scheme with Revocation Capability. The KIPS Transactions PartC, 2005, 12C, 941-948.	0.2	0
63	The Related-Key Rectangle Attack â€“ Application to SHACAL-1. Lecture Notes in Computer Science, 2004, , 123-136.	1.3	46
64	Convergence of Jump-Diffusion Modelsto the Blackâ€“Scholes Model. Stochastic Analysis and Applications, 2003, 21, 141-160.	1.5	6
65	A Concrete Security Analysis for 3GPP-MAC. Lecture Notes in Computer Science, 2003, , 154-169.	1.3	8
66	Efficient Oblivious Transfer in the Bounded-Storage Model. Lecture Notes in Computer Science, 2002, , 143-159.	1.3	7
67	Pseudorandomness of MISTY-Type Transformations and the Block Cipher KASUMI. Lecture Notes in Computer Science, 2001, , 60-73.	1.3	10
68	Provable Security of KASUMI and 3GPP Encryption Mode f8. Lecture Notes in Computer Science, 2001, , 255-271.	1.3	14