

Edward Dawson

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/3320795/publications.pdf>

Version: 2024-02-01

117
papers

1,824
citations

279487

23
h-index

315357

38
g-index

125
all docs

125
docs citations

125
times ranked

848
citing authors

#	ARTICLE	IF	CITATIONS
1	Multistage secret sharing based on one-way function. Electronics Letters, 1994, 30, 1591-1592.	0.5	134
2	Twisted Edwards Curves Revisited. Lecture Notes in Computer Science, 2008, , 326-343.	1.0	126
3	Heuristic design of cryptographically strong balanced Boolean functions. Lecture Notes in Computer Science, 1998, , 489-499.	1.0	91
4	A novel identity-based strong designated verifier signature scheme. Journal of Systems and Software, 2009, 82, 270-273.	3.3	89
5	Multisecret-sharing scheme based on one-way function. Electronics Letters, 1995, 31, 93-95.	0.5	82
6	A computer package for measuring the strength of encryption algorithms. Computers and Security, 1994, 13, 687-697.	4.0	74
7	Bit-Pattern Based Integral Attack. Lecture Notes in Computer Science, 2008, , 363-381.	1.0	55
8	PKI, elliptic curve cryptography, and digital signatures. Computers and Security, 1999, 18, 47-66.	4.0	47
9	The breadth of Shamir's secret-sharing scheme. Computers and Security, 1994, 13, 69-78.	4.0	46
10	Identity-based strong designated verifier signature schemes: Attacks and new construction. Computers and Electrical Engineering, 2009, 35, 49-53.	3.0	45
11	Multiplicative Homomorphic E-Voting. Lecture Notes in Computer Science, 2004, , 61-72.	1.0	35
12	Simple and Efficient Shuffling with Provable Correctness and ZK Privacy. Lecture Notes in Computer Science, 2005, , 188-204.	1.0	33
13	Dragon: A Fast Word Based Stream Cipher. Lecture Notes in Computer Science, 2005, , 33-50.	1.0	31
14	A Correct, Private, and Efficient Mix Network. Lecture Notes in Computer Science, 2004, , 439-454.	1.0	30
15	Fast Correlation Attacks on the Summation Generator. Journal of Cryptology, 2000, 13, 245-262.	2.1	29
16	Graph theory based representation of building information models for access control applications. Automation in Construction, 2016, 68, 44-51.	4.8	29
17	The LILI-II Keystream Generator. Lecture Notes in Computer Science, 2002, , 25-39.	1.0	29
18	AUTOMATED CRYPTANALYSIS OF XOR PLAINTEXT STRINGS. Cryptologia, 1996, 20, 165-181.	0.4	28

#	ARTICLE	IF	CITATIONS
19	Boolean Function Design Using Hill Climbing Methods. Lecture Notes in Computer Science, 1999, , 1-11.	1.0	28
20	New Formulae for Efficient Elliptic Curve Arithmetic. , 2007, , 138-151.		28
21	Batch zero-knowledge proof and verification and its applications. ACM Transactions on Information and System Security, 2007, 10, 6.	4.5	27
22	Generalized inversion attack on nonlinear filter generators. IEEE Transactions on Computers, 2000, 49, 1100-1109.	2.4	24
23	Multi-objective optimisation of bijective s-boxes. New Generation Computing, 2005, 23, 201-218.	2.5	23
24	A Three Phased Schema for Sealed Bid Auction System Design. Lecture Notes in Computer Science, 2000, , 412-426.	1.0	23
25	Existence of Generalized Inverse of Linear Transformations over Finite Fields. Finite Fields and Their Applications, 1998, 4, 307-315.	0.6	21
26	Jacobi Quartic Curves Revisited. Lecture Notes in Computer Science, 2009, , 452-468.	1.0	21
27	Specification and design of advanced authentication and authorization services. Computer Standards and Interfaces, 2005, 27, 467-478.	3.8	19
28	Batch verification of validity of bids in homomorphic e-auction. Computer Communications, 2006, 29, 2798-2805.	3.1	18
29	DIVIDE AND CONQUER ATTACKS ON CERTAIN CLASSES OF STREAM CIPHERS. Cryptologia, 1994, 18, 25-40.	0.4	17
30	Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN. Communications in Computer and Information Science, 2016, , 15-26.	0.4	16
31	A PARALLEL GENETIC ALGORITHM FOR CRYPTANALYSIS OF THE POLYALPHABETIC SUBSTITUTION CIPHER. Cryptologia, 1997, 21, 129-138.	0.4	15
32	New Concepts in Evolutionary Search for Boolean Functions in Cryptology. Computational Intelligence, 2004, 20, 463-474.	2.1	15
33	Correlation immunity and resiliency of symmetric Boolean functions. Theoretical Computer Science, 2004, 312, 321-335.	0.5	15
34	An Approach to Access Control under Uncertainty. , 2011, , .		15
35	A Public Key Cryptosystem Based On A Subgroup Membership Problem. Designs, Codes, and Cryptography, 2005, 36, 301-316.	1.0	13
36	Modification and optimisation of a shuffling scheme: stronger security, formal analysis and higher efficiency. International Journal of Information Security, 2011, 10, 33-47.	2.3	13

#	ARTICLE	IF	CITATIONS
37	A policy model for access control using building information models. International Journal of Critical Infrastructure Protection, 2018, 23, 1-10.	2.9	13
38	Batch Verification for Equality of Discrete Logarithms and Threshold Decryptions. Lecture Notes in Computer Science, 2004, , 494-508.	1.0	12
39	The efficiency of solving multiple discrete logarithm problems and the implications for the security of fixed elliptic curves. International Journal of Information Security, 2004, 3, 86-98.	2.3	11
40	An Authorization Framework using Building Information Models. Computer Journal, 2012, 55, 1244-1264.	1.5	11
41	Efficient Implementation of Relative Bid Privacy in Sealed-Bid Auction. Lecture Notes in Computer Science, 2004, , 244-256.	1.0	11
42	Shared Secret Reconstruction. Designs, Codes, and Cryptography, 1998, 14, 221-237.	1.0	10
43	Ciphertext Comparison, a New Solution to the Millionaire Problem. Lecture Notes in Computer Science, 2005, , 84-96.	1.0	10
44	Key agreement scheme based on generalised inverses of matrices. Electronics Letters, 1997, 33, 1210.	0.5	9
45	A Method for Measuring Entropy of Symmetric Cipher Key Generators. Computers and Security, 1998, 17, 177-184.	4.0	9
46	On a taxonomy of delegation. Computers and Security, 2010, 29, 565-579.	4.0	9
47	Random Fault Attacks on a Class of Stream Ciphers. Security and Communication Networks, 2019, 2019, 1-12.	1.0	9
48	A Public Key Cryptosystem Based on the Subgroup Membership Problem. Lecture Notes in Computer Science, 2001, , 352-363.	1.0	9
49	Key Derivation Function: The SCKDF Scheme. IFIP Advances in Information and Communication Technology, 2013, , 125-138.	0.5	9
50	Key management in a non-trusted distributed environment. Future Generation Computer Systems, 2000, 16, 319-329.	4.9	8
51	Virtual certificates and synthetic certificates: new paradigms for improving public key validation. Computer Communications, 2003, 26, 1826-1838.	3.1	8
52	Investigating Cube Attacks on the Authenticated Encryption Stream Cipher MORUS. , 2017, , .		8
53	Non-interactive Auction Scheme with Strong Privacy. Lecture Notes in Computer Science, 2003, , 407-420.	1.0	8
54	Efficient Bid Validity Check in ElGamal-Based Sealed-Bid E-Auction. , 2007, , 209-224.		8

#	ARTICLE	IF	CITATIONS
55	Micropayments for Wireless Communications. Lecture Notes in Computer Science, 2001, , 192-205.	1.0	8
56	Discrete optimisation and fast correlation attacks. Lecture Notes in Computer Science, 1996, , 186-200.	1.0	7
57	A fast correlation attack on multiplexer generators. Information Processing Letters, 1999, 70, 89-93.	0.4	7
58	A novel nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Computers and Electrical Engineering, 2009, 35, 9-17.	3.0	7
59	A Framework for Security Analysis of Key Derivation Functions. Lecture Notes in Computer Science, 2012, , 199-216.	1.0	7
60	COMBINATORIAL OPTIMIZATION AND THE KNAPSACK CIPHER. Cryptologia, 1996, 20, 85-93.	0.4	6
61	An Efficient and Verifiable Solution to the Millionaire Problem. Lecture Notes in Computer Science, 2005, , 51-66.	1.0	6
62	Towards a Game Theoretic Authorisation Model. Lecture Notes in Computer Science, 2010, , 208-219.	1.0	6
63	Budget-aware Role Based Access Control. Computers and Security, 2013, 35, 37-50.	4.0	6
64	Fault Attacks on the Authenticated Encryption Stream Cipher MORUS. Cryptography, 2018, 2, 4.	1.4	6
65	Physical Access Control Administration Using Building Information Models. Lecture Notes in Computer Science, 2012, , 236-250.	1.0	6
66	A Novel Range Test. Lecture Notes in Computer Science, 2006, , 247-258.	1.0	6
67	Finding state collisions in the authenticated encryption stream cipher ACORN. , 2016, , .		5
68	Fault attacks on Tiaoxin-346. , 2018, , .		5
69	A Mobile Agent System Providing Offer Privacy. Lecture Notes in Computer Science, 2004, , 301-312.	1.0	5
70	Rekeying Issues in the MUGI Stream Cipher. Lecture Notes in Computer Science, 2006, , 175-188.	1.0	5
71	Testing for randomness in stream ciphers using the binary derivative. Statistics and Computing, 1995, 5, 307-310.	0.8	4
72	Klein Bottle Routing: An Alternative to Onion Routing and Mix Network. Lecture Notes in Computer Science, 2006, , 296-309.	1.0	4

#	ARTICLE	IF	CITATIONS
73	An exploration of affine group laws for elliptic curves. <i>Journal of Mathematical Cryptology</i> , 2011, 5, 1-50.	0.4	4
74	Consistency of User Attribute in Federated Systems. <i>Lecture Notes in Computer Science</i> , 2007, , 165-177.	1.0	4
75	Analysis of Indirect Message Injection for MAC Generation Using Stream Ciphers. <i>Lecture Notes in Computer Science</i> , 2012, , 138-151.	1.0	4
76	On the security of self-synchronous ciphers. <i>Lecture Notes in Computer Science</i> , 1997, , 159-170.	1.0	3
77	BAAI: biometric authentication and authorization infrastructure. , 2003, , .		3
78	A Fault-based Attack on AEZ v4.2. , 2017, , .		3
79	Key Recovery System for the Commercial Environment. <i>Lecture Notes in Computer Science</i> , 2000, , 149-162.	1.0	3
80	Cryptanalysis of tree-structured ciphers. <i>Electronics Letters</i> , 1994, 30, 941-942.	0.5	2
81	Forgery attacks on ++AE authenticated encryption mode. , 2016, , .		2
82	Secure Selection Protocols. <i>Lecture Notes in Computer Science</i> , 2000, , 132-146.	1.0	2
83	On a Taxonomy of Delegation. <i>IFIP Advances in Information and Communication Technology</i> , 2009, , 353-363.	0.5	2
84	Offer Privacy in Mobile Agents Using Conditionally Anonymous Digital Signatures. <i>Lecture Notes in Computer Science</i> , 2004, , 132-141.	1.0	2
85	A Novel Method to Maintain Privacy in Mobile Agent Applications. <i>Lecture Notes in Computer Science</i> , 2005, , 247-260.	1.0	2
86	Linearity within the SMS4 Block Cipher. <i>Lecture Notes in Computer Science</i> , 2010, , 248-265.	1.0	2
87	Message collision in block ciphers with message authentication. <i>Computers and Security</i> , 1993, 12, 781-787.	4.0	1
88	Signature Scheme for Controlled Environments. <i>Lecture Notes in Computer Science</i> , 1999, , 119-134.	1.0	1
89	The Security of Fixed versus Random Elliptic Curves in Cryptography. <i>Lecture Notes in Computer Science</i> , 2003, , 55-66.	1.0	1
90	Optimal Budget Allocation in Budget-based Access Control. , 2011, , .		1

#	ARTICLE	IF	CITATIONS
91	Slide attacks on the Sifinks stream cipher. , 2012, , .		1
92	State convergence and keyspace reduction of the Mixer stream cipher. Journal of Discrete Mathematical Sciences and Cryptography, 2012, 15, 89-104.	0.5	1
93	Stream cipher based key derivation function. International Journal of Security and Networks, 2017, 12, 70.	0.1	1
94	Fault Attacks on XEX Mode with Application to Certain Authenticated Encryption Modes. Lecture Notes in Computer Science, 2017, , 285-305.	1.0	1
95	A General Model for MAC Generation Using Direct Injection. Lecture Notes in Computer Science, 2013, , 198-215.	1.0	1
96	Differential Random Fault Attacks on Certain CAESAR Stream Ciphers. Lecture Notes in Computer Science, 2020, , 297-315.	1.0	1
97	Hybrid Key Escrow: A New Paradigm,. Computers and Security, 2001, 21, 77-92.	4.0	0
98	Statistical Weakness of Multiplexed Sequences. Finite Fields and Their Applications, 2002, 8, 420-433.	0.6	0
99	Compliant cryptologic protocols. International Journal of Information Security, 2002, 1, 189-202.	2.3	0
100	The Dragon Stream Cipher: Design, Analysis, and Implementation Issues. Lecture Notes in Computer Science, 2008, , 20-38.	1.0	0
101	Algebraic analysis of the SSS stream cipher. , 2011, , .		0
102	State convergence and the effectiveness of time-memory-data tradeoffs. , 2011, , .		0
103	Indirect message injection for MAC generation. Journal of Mathematical Cryptology, 2013, 7, .	0.4	0
104	A fundamental flaw in the ++AE authenticated encryption mode. Journal of Mathematical Cryptology, 2018, 12, 37-42.	0.4	0
105	SPCC: a security policy compliance checker plug-in for YAWL. International Journal of Business Process Integration and Management, 2018, 9, 22.	0.2	0
106	PAIS Access Control Model Characteristics Analysis. , 2018, , .		0
107	Fault analysis of AEZ. Concurrency Computation Practice and Experience, 2019, 31, e4785.	1.4	0
108	Cryptographic Salt: A Countermeasure against Denial-of-Service Attacks. Lecture Notes in Computer Science, 2001, , 334-343.	1.0	0

#	ARTICLE	IF	CITATIONS
109	A Survey of Divide and Conquer Attacks on Certain Irregularly Clocked Stream Ciphers. , 2001, , 165-185.		0
110	Ensuring Fast Implementations of Symmetric Ciphers on the Intel Pentium 4 and Beyond. Lecture Notes in Computer Science, 2006, , 52-63.	1.0	0
111	A Model for Constraint and Delegation Management. Lecture Notes in Computer Science, 2011, , 362-371.	1.0	0
112	Weaknesses in the Initialisation Process of the Common Scrambling Algorithm Stream Cipher. Lecture Notes in Computer Science, 2014, , 220-233.	1.0	0
113	Flaws in the Initialisation Process of Stream Ciphers. , 2015, , 19-49.		0
114	Stream cipher based key derivation function. International Journal of Security and Networks, 2017, 12, 70.	0.1	0
115	On the Security Analysis of Weak Cryptographic Primitive Based Key Derivation Function. Lecture Notes in Electrical Engineering, 2017, , 231-240.	0.3	0
116	Advances in security research in the Asiacrypt region. Communications of the ACM, 2020, 63, 76-81.	3.3	0
117	Sealed-Bid Micro Auctions. , 2006, , 246-257.		0