

John Kelsey

List of Publications by Citations

Source: <https://exaly.com/author-pdf/4036615/john-kelsey-publications-by-citations.pdf>

Version: 2024-04-28

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

42
papers

1,662
citations

19
h-index

40
g-index

42
ext. papers

1,872
ext. citations

1.1
avg, IF

4.35
L-index

#	Paper	IF	Citations
42	Secure audit logs to support computer forensics. <i>ACM Transactions on Information and System Security</i> , 1999 , 2, 159-176		218
41	Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work. <i>Lecture Notes in Computer Science</i> , 2005 , 474-490	0.9	158
40	Improved Cryptanalysis of Rijndael. <i>Lecture Notes in Computer Science</i> , 2001 , 213-230	0.9	154
39	Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. <i>Lecture Notes in Computer Science</i> , 1996 , 237-251	0.9	118
38	Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. <i>Lecture Notes in Computer Science</i> , 1997 , 233-246	0.9	105
37	Herding Hash Functions and the Nostradamus Attack. <i>Lecture Notes in Computer Science</i> , 2006 , 183-200	0.9	94
36	Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. <i>Lecture Notes in Computer Science</i> , 2001 , 75-93	0.9	91
35	Cryptanalytic Attacks on Pseudorandom Number Generators. <i>Lecture Notes in Computer Science</i> , 1998 , 168-188	0.9	80
34	Side channel cryptanalysis of product ciphers. <i>Lecture Notes in Computer Science</i> , 1998 , 97-110	0.9	79
33	Unbalanced Feistel networks and block cipher design. <i>Lecture Notes in Computer Science</i> , 1996 , 121-144	0.9	75
32	Recommendation for the entropy sources used for random bit generation		55
31	Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive. <i>Lecture Notes in Computer Science</i> , 2003 , 330-346	0.9	54
30	Protocol interactions and the chosen protocol attack. <i>Lecture Notes in Computer Science</i> , 1998 , 91-104	0.9	45
29	Building PRFs from PRPs. <i>Lecture Notes in Computer Science</i> , 1998 , 370-389	0.9	43
28	Compression and Information Leakage of Plaintext. <i>Lecture Notes in Computer Science</i> , 2002 , 263-276	0.9	36
27	Second Preimage Attacks on Dithered Hash Functions 2008 , 270-288		33
26	Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator. <i>Lecture Notes in Computer Science</i> , 2000 , 13-33	0.9	28

25	Mod n Cryptanalysis, with Applications against RC5P and M6. <i>Lecture Notes in Computer Science</i> , 1999 , 139-155	0.9	22
24	Secure applications of low-entropy keys. <i>Lecture Notes in Computer Science</i> , 1998 , 121-134	0.9	21
23	SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash		19
22	Linear-XOR and Additive Checksums Don't Protect Damgård-Merkle Hashes from Generic Attacks. <i>Lecture Notes in Computer Science</i> , 2008 , 36-51	0.9	18
21	New Second-Preimage Attacks on Hash Functions. <i>Journal of Cryptology</i> , 2016 , 29, 657-696	2.1	15
20	On hash functions using checksums. <i>International Journal of Information Security</i> , 2010 , 9, 137-151	2.8	14
19	Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård. <i>Lecture Notes in Computer Science</i> , 2009 , 393-414	0.9	14
18	Collisions and Near-Collisions for Reduced-Round Tiger. <i>Lecture Notes in Computer Science</i> , 2006 , 111-125.	0.9	14
17	Remote auditing of software outputs using a trusted coprocessor. <i>Future Generation Computer Systems</i> , 1997 , 13, 9-18	7.5	12
16	Cryptanalysis of the cellular message encryption algorithm. <i>Lecture Notes in Computer Science</i> , 1997 , 526-537	0.9	10
15	Predictive Models for Min-entropy Estimation. <i>Lecture Notes in Computer Science</i> , 2015 , 373-392	0.9	8
14	Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness. <i>Lecture Notes in Computer Science</i> , 2017 , 410-425	0.9	6
13	Attacking Paper-Based E2E Voting Systems. <i>Lecture Notes in Computer Science</i> , 2010 , 370-387	0.9	5
12	On the Twofish Key Schedule. <i>Lecture Notes in Computer Science</i> , 1999 , 27-42	0.9	4
11	Key-Schedule Cryptanalysis of DEAL. <i>Lecture Notes in Computer Science</i> , 2000 , 118-134	0.9	3
10	Automatic event-stream notarization using digital signatures. <i>Lecture Notes in Computer Science</i> , 1997 , 155-169	0.9	3
9	Cryptanalysis of TWOPRIME. <i>Lecture Notes in Computer Science</i> , 1998 , 32-48	0.9	3
8	Design Principles for True Random Number Generators for Security Applications 2019 ,		2

7	Conditional purchase orders 1997 ,		2
6	Cryptanalysis of SPEED. <i>Lecture Notes in Computer Science</i> , 1999 , 319-338	0.9	1
5	TMPS: Ticket-Mediated Password Strengthening. <i>Lecture Notes in Computer Science</i> , 2020 , 225-253	0.9	0
4	The New Randomness Beacon Format Standard: An Exercise in Limiting the Power of a Trusted Third Party. <i>Lecture Notes in Computer Science</i> , 2018 , 164-184	0.9	0
3	Cryptanalysis of SPEED. <i>Lecture Notes in Computer Science</i> , 1998 , 309-310	0.9	
2	Secure Authentication with Multiple Parallel Keys. <i>Lecture Notes in Computer Science</i> , 2000 , 150-156	0.9	
1	Distributed proctoring. <i>Lecture Notes in Computer Science</i> , 1996 , 172-182	0.9	