John Kelsey

List of Publications by Year in Descending Order

Source: https://exaly.com/author-pdf/4036615/john-kelsey-publications-by-year.pdf
Version: 2024-04-28

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	TMPS: Ticket-Mediated Password Strengthening. *Lecture Notes in Computer Science*, **2020**, 225-253	0.9	0
41	Design Principles for True Random Number Generators for Security Applications **2019**,		2
40	The New Randomness Beacon Format Standard: An Exercise in Limiting the Power of a Trusted Third Party. *Lecture Notes in Computer Science*, **2018**, 164-184	0.9	0
39	Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness. *Lecture Notes in Computer Science*, **2017**, 410-425	0.9	6
38	New Second-Preimage Attacks on Hash Functions. *Journal of Cryptology*, **2016**, 29, 657-696	2.1	15
37	Predictive Models for Min-entropy Estimation. *Lecture Notes in Computer Science*, **2015**, 373-392	0.9	8
36	On hash functions using checksums. *International Journal of Information Security*, **2010**, 9, 137-151	2.8	14
35	Attacking Paper-Based E2E Voting Systems. *Lecture Notes in Computer Science*, **2010**, 370-387	0.9	5
34	Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damg��d. *Lecture Notes in Computer Science*, **2009**, 393-414	0.9	14
33	Linear-XOR and Additive Checksums Don� Protect Damg��d-Merkle Hashes from Generic Attacks. *Lecture Notes in Computer Science*, **2008**, 36-51	0.9	18
32	Second Preimage Attacks on Dithered Hash Functions **2008**, 270-288		33
31	Herding Hash Functions and the Nostradamus Attack. *Lecture Notes in Computer Science*, **2006**, 183-200	0.9	94
30	Collisions and Near-Collisions for Reduced-Round Tiger. *Lecture Notes in Computer Science*, **2006**, 111-125	0.9	14
29	Second Preimages on n-Bit Hash Functions for Much Less than 2n Work. *Lecture Notes in Computer Science*, **2005**, 474-490	0.9	158
28	Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive. *Lecture Notes in Computer Science*, **2003**, 330-346	0.9	54
27	Compression and Information Leakage of Plaintext. *Lecture Notes in Computer Science*, **2002**, 263-276	0.9	36
26	Improved Cryptanalysis of Rijndael. *Lecture Notes in Computer Science*, **2001**, 213-230	0.9	154

(1997-2001)

25	Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. *Lecture Notes in Computer Science*, **2001**, 75-93	0.9	91
24	Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator. *Lecture Notes in Computer Science*, **2000**, 13-33	0.9	28
23	Secure Authentication with Multiple Parallel Keys. *Lecture Notes in Computer Science*, **2000**, 150-156	0.9	
22	Key-Schedule Cryptanalysis of DEAL. *Lecture Notes in Computer Science*, **2000**, 118-134	0.9	3
21	Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security*, **1999**, 2, 159-176		218
20	On the Twofish Key Schedule. *Lecture Notes in Computer Science*, **1999**, 27-42	0.9	4
19	Mod n Cryptanalysis, with Applications against RC5P and M6. *Lecture Notes in Computer Science*, **1999**, 139-155	0.9	22
18	Cryptanalysis of SPEED. *Lecture Notes in Computer Science*, **1999**, 319-338	0.9	1
17	Protocol interactions and the chosen protocol attack. *Lecture Notes in Computer Science*, **1998**, 91-104	0.9	45
16	Side channel cryptanalysis of product ciphers. *Lecture Notes in Computer Science*, **1998**, 97-110	0.9	79
15	Cryptanalytic Attacks on Pseudorandom Number Generators. *Lecture Notes in Computer Science*, **1998**, 168-188	0.9	80
14	Cryptanalysis of SPEED. *Lecture Notes in Computer Science*, **1998**, 309-310	0.9	
13	Secure applications of low-entropy keys. *Lecture Notes in Computer Science*, **1998**, 121-134	0.9	21
12	Building PRFs from PRPs. *Lecture Notes in Computer Science*, **1998**, 370-389	0.9	43
11	Cryptanalysis of TWOPRIME. *Lecture Notes in Computer Science*, **1998**, 32-48	0.9	3
10	Related-key cryptanalysis of 3-WAY, Biham-DES,CAST, DES-X, NewDES, RC2, and TEA. *Lecture Notes in Computer Science*, **1997**, 233-246	0.9	105
9	Cryptanalysis of the cellular message encryption algorithm. *Lecture Notes in Computer Science*, **1997** , 526-537	0.9	10
8	Remote auditing of software outputs using a trusted coprocessor. *Future Generation Computer Systems*, **1997**, 13, 9-18	7.5	12

7	Conditional purchase orders **1997**,		2
6	Automatic event-stream notarization using digital signatures. *Lecture Notes in Computer Science*, **1997**, 155-169	0.9	3
5	Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. *Lecture Notes in Computer Science*, **1996**, 237-251	0.9	118
4	Distributed proctoring. *Lecture Notes in Computer Science*, **1996**, 172-182	0.9	
3	Unbalanced Feistel networks and block cipher design. *Lecture Notes in Computer Science*, **1996**, 121-144	0.9	75
2	SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash		19
1	Recommendation for the entropy sources used for random bit generation		55