John Kelsey

List of Publications by Citations

42	1,662	19	40
papers	citations	h-index	g-index

42	1,872	1.1	4.35
ext. papers	ext. citations	avg, IF	L-index

#	Paper	IF	Citations
42	Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security*, **1999**, 2, 159-176		218
41	Second Preimages on n-Bit Hash Functions for Much Less than 2n Work. *Lecture Notes in Computer Science*, **2005**, 474-490	0.9	158
40	Improved Cryptanalysis of Rijndael. *Lecture Notes in Computer Science*, **2001**, 213-230	0.9	154
39	Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. *Lecture Notes in Computer Science*, **1996**, 237-251	0.9	118
38	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
37	Herding Hash Functions and the Nostradamus Attack. *Lecture Notes in Computer Science*, **2006**, 183-200	0.9	94
36	Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. *Lecture Notes in Computer Science*, **2001**, 75-93	0.9	91
35	Cryptanalytic Attacks on Pseudorandom Number Generators. *Lecture Notes in Computer Science*, **1998**, 168-188	0.9	80
34	Side channel cryptanalysis of product ciphers. *Lecture Notes in Computer Science*, **1998**, 97-110	0.9	79
33	Unbalanced Feistel networks and block cipher design. *Lecture Notes in Computer Science*, **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. *Lecture Notes in Computer Science*, **2003**, 330-346	0.9	54
30	Protocol interactions and the chosen protocol attack. *Lecture Notes in Computer Science*, **1998**, 91-104	0.9	45
29	Building PRFs from PRPs. *Lecture Notes in Computer Science*, **1998**, 370-389	0.9	43
28	Compression and Information Leakage of Plaintext. *Lecture Notes in Computer Science*, **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. *Lecture Notes in Computer Science*, **2000**, 13-33	0.9	28

25	Mod n Cryptanalysis, with Applications against RC5P and M6. *Lecture Notes in Computer Science*, **1999**, 139-155	0.9	22
24	Secure applications of low-entropy keys. *Lecture Notes in Computer Science*, **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. *Lecture Notes in Computer Science*, **2008**, 36-51	0.9	18
21	New Second-Preimage Attacks on Hash Functions. *Journal of Cryptology*, **2016**, 29, 657-696	2.1	15
20	On hash functions using checksums. *International Journal of Information Security*, **2010**, 9, 137-151	2.8	14
19	Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård. *Lecture Notes in Computer Science*, **2009**, 393-414	0.9	14
18	Collisions and Near-Collisions for Reduced-Round Tiger. *Lecture Notes in Computer Science*, **2006**, 111-125	0.9	14
17	Remote auditing of software outputs using a trusted coprocessor. *Future Generation Computer Systems*, **1997**, 13, 9-18	7.5	12
16	Cryptanalysis of the cellular message encryption algorithm. *Lecture Notes in Computer Science*, **1997**, 526-537	0.9	10
15	Predictive Models for Min-entropy Estimation. *Lecture Notes in Computer Science*, **2015**, 373-392	0.9	8
14	Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness. *Lecture Notes in Computer Science*, **2017**, 410-425	0.9	6
13	Attacking Paper-Based E2E Voting Systems. *Lecture Notes in Computer Science*, **2010**, 370-387	0.9	5
12	On the Twofish Key Schedule. *Lecture Notes in Computer Science*, **1999**, 27-42	0.9	4
11	Key-Schedule Cryptanalysis of DEAL. *Lecture Notes in Computer Science*, **2000**, 118-134	0.9	3
10	Automatic event-stream notarization using digital signatures. *Lecture Notes in Computer Science*, **1997**, 155-169	0.9	3
9	Cryptanalysis of TWOPRIME. *Lecture Notes in Computer Science*, **1998**, 32-48	0.9	3
8	Design Principles for True Random Number Generators for Security Applications **2019**,		2