Adi Shamir

List of Publications by Citations

Source: https://exaly.com/author-pdf/4992034/adi-shamir-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.

64 papers	12,448 citations	29 h-index	64 g-index
64 ext. papers	14,755 ext. citations	1.4 avg, IF	6.65 L-index

#	Paper	IF	Citations
64	How to share a secret. *Communications of the ACM*, **1979**, 22, 612-613	2.5	7167
63	Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, **1991**, 4, 3-72	2.1	1216
62	Differential fault analysis of secret key cryptosystems. *Lecture Notes in Computer Science*, **1997**, 513-525	0.9	658
61	Differential Cryptanalysis of the Data Encryption Standard **1993**,		459
60	Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. *Lecture Notes in Computer Science*, **2000**, 392-407	0.9	288
59	Efficient Cache Attacks on AES, and Countermeasures. *Journal of Cryptology*, **2010**, 23, 37-71	2.1	241
58	The LSD Broadcast Encryption Scheme. *Lecture Notes in Computer Science*, **2002**, 47-60	0.9	188
57	Cube Attacks on Tweakable Black Box Polynomials. *Lecture Notes in Computer Science*, **2009**, 278-299	0.9	187
56	IoT Goes Nuclear: Creating a ZigBee Chain Reaction **2017**,		179
55	Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. *Lecture Notes in Computer Science*, **2000**, 1-13	0.9	151
54	On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, **1983**, 1, 38-44	1.1	137
53	RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. *Lecture Notes in Computer Science*, **2014**, 444-461	0.9	134
52	Real Time Cryptanalysis of A5/1 on a PC. *Lecture Notes in Computer Science*, **2001**, 1-18	0.9	128
51	A $T = O(2^{n/2})$, $S = O(2^{n/4})$ Algorithm for Certain NP-Complete Problems. *SIAM Journal on Computing*, **1981**, 10, 456-464	1.1	118
50	Differential Cryptanalysis of the Full 16-round DES **1992**, 487-496		115
49	Extended Functionality Attacks on IoT Devices: The Case of Smart Lights **2016**,		92
48	Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium. *Lecture Notes in Computer Science*, **2009**, 1-22	0.9	84

(2014-1999)

47	Miss in the Middle Attacks on IDEA and Khufu. *Lecture Notes in Computer Science*, **1999**, 124-138	0.9	83
46	Minimalism in Cryptography: The Even-Mansour Scheme Revisited. *Lecture Notes in Computer Science*, **2012**, 336-354	0.9	82
45	Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. *Lecture Notes in Computer Science*, **2010**, 299-319	0.9	62
44	Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. *Journal of Cryptology*, **2005**, 18, 291-311	2.1	58
43	Remote Password Extraction from RFID Tags. *IEEE Transactions on Computers*, **2007**, 56, 1292-1296	2.5	46
42	Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems. *Lecture Notes in Computer Science*, **2012**, 719-740	0.9	42
41	Efficient Factoring Based on Partial Information **1985**, 31-34		37
40	Structural Cryptanalysis of SASAS. *Journal of Cryptology*, **2010**, 23, 505-518	2.1	35
39	Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer **1991**, 156-171		35
38	Second Preimage Attacks on Dithered Hash Functions **2008**, 270-288		33
37	Improved Attacks on Full GOST. *Lecture Notes in Computer Science*, **2012**, 9-28	0.9	32
36	A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *Journal of Cryptology*, **2014**, 27, 824-849	2.1	31
35	Acoustic Cryptanalysis. *Journal of Cryptology*, **2017**, 30, 392-443	2.1	28
34	The Theoretical Aspects of the Optimal Fixedpoint. *SIAM Journal on Computing*, **1976**, 5, 414-426	1.1	28
33	Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2. *Lecture Notes in Computer Science*, **2013**, 337-356	0.9	24
32	Differential Cryptanalysis of Feal and N-Hash **1991**, 1-16		23
31	Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. *Lecture Notes in Computer Science*, **1999**, 362-375	0.9	22
30	Improved Practical Attacks on Round-Reduced Keccak. *Journal of Cryptology*, **2014**, 27, 183-209	2.1	19

29	Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *Journal of Cryptology*, **2015**, 28, 397-422	2.1	17
28	Applying cube attacks to stream ciphers in realistic scenarios. *Cryptography and Communications*, **2012**, 4, 217-232	1.1	17
27	Slidex Attacks on the Even□Mansour Encryption Scheme. *Journal of Cryptology*, **2015**, 28, 1-28	2.1	15
26	New Second-Preimage Attacks on Hash Functions. *Journal of Cryptology*, **2016**, 29, 657-696	2.1	15
25	Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. *Lecture Notes in Computer Science*, **2014**, 439-457	0.9	13
24	Key Recovery Attacks on Iterated Even□Mansour Encryption Schemes. *Journal of Cryptology*, **2016**, 29, 697-728	2.1	10
23	How to find a battleship. *Networks*, **1989**, 19, 361-371	1.6	10
22	The convergence of functions to fixedpoints of recursive definitions. *Theoretical Computer Science*, **1978**, 6, 109-141	1.1	10
21	New Attacks on IDEA with at Least 6 Rounds. *Journal of Cryptology*, **2015**, 28, 209-239	2.1	8
20	. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 415-430	8	8
19	RFID Authentication Efficient Proactive Information Security within Computational Security. *Theory of Computing Systems*, **2011**, 48, 132-149	0.6	8
18	The Retracing Boomerang Attack. *Lecture Notes in Computer Science*, **2020**, 280-309	0.9	8
17	Length-based cryptanalysis: the case of Thompson's group. *Journal of Mathematical Cryptology*, **2007**, 1,	0.6	7
16	Bug Attacks. *Journal of Cryptology*, **2016**, 29, 775-805	2.1	5
15	Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities. *Journal of Cryptology*, **2020**, 33, 1003-1043	2.1	5
14	How to Eat Your Entropy and Have it Too: Optimal Recovery Strategies for Compromised RNGs. *Algorithmica*, **2017**, 79, 1196-1232	0.9	4
13	Almost universal forgery attacks on AES-based MAC□. *Designs, Codes, and Cryptography*, **2015**, 76, 431-449	1.2	4
12	Generic Analysis of Small Cryptographic Leaks **2010**,		4

List of Publications

11	Improved Top-Down Techniques in Differential Cryptanalysis. *Lecture Notes in Computer Science*, **2015**, 139-156	0.9	4
10	Reflections on slide with a twist attacks. *Designs, Codes, and Cryptography*, **2015**, 77, 633-651	1.2	3
9	Improved Related-key Attacks on DESX and DESX+. *Cryptologia*, **2008**, 32, 13-22	0.9	3
8	Efficient Dissection of Bicomposite Problems with Cryptanalytic Applications. *Journal of Cryptology*, **2019**, 32, 1448-1490	2.1	2
7	New Slide Attacks on Almost Self-similar Ciphers. *Lecture Notes in Computer Science*, **2020**, 250-279	0.9	2
6	Detecting Spying Drones. *IEEE Security and Privacy*, **2021**, 19, 65-73	2	2
5	Dissection. *Communications of the ACM*, **2014**, 57, 98-105	2.5	1
4	Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64. *Lecture Notes in Computer Science*, **2015**, 390-410	0.9	1
3	Tight Bounds on Online Checkpointing Algorithms. *ACM Transactions on Algorithms*, **2020**, 16, 1-22	1.2	
2	A New Approach to Recursive Programs **1977**, 103-124		
1	Game of Drones - Detecting Spying Drones Using Time Domain Analysis. *Lecture Notes in Computer Science*, **2021**, 128-144	0.9	