Adi Shamir

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4992034/publications.pdf

Version: 2024-02-01

63 papers	17,307 citations	249298 26 h-index	190340 53 g-index
64 all docs	64 docs citations	64 times ranked	7393 citing authors

#	Article	IF	Citations
1	Game of Drones - Detecting Spying Drones Using Time Domain Analysis. Lecture Notes in Computer Science, 2021, , 128-144.	1.0	1
2	Detecting Spying Drones. IEEE Security and Privacy, 2021, 19, 65-73.	1.5	8
3	Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities. Journal of Cryptology, 2020, 33, 1003-1043.	2.1	14
4	New Slide Attacks on Almost Self-similar Ciphers. Lecture Notes in Computer Science, 2020, , 250-279.	1.0	2
5	The Retracing Boomerang Attack. Lecture Notes in Computer Science, 2020, , 280-309.	1.0	18
6	Tight Bounds on Online Checkpointing Algorithms. ACM Transactions on Algorithms, 2020, 16, 1-22.	0.9	0
7	Xerox Day Vulnerability. IEEE Transactions on Information Forensics and Security, 2019, 14, 415-430.	4.5	12
8	Efficient Dissection of Bicomposite Problems with Cryptanalytic Applications. Journal of Cryptology, 2019, 32, 1448-1490.	2.1	3
9	Acoustic Cryptanalysis. Journal of Cryptology, 2017, 30, 392-443.	2.1	60
10	How to Eat Your Entropy and Have it Too: Optimal Recovery Strategies for Compromised RNGs. Algorithmica, 2017, 79, 1196-1232.	1.0	6
11	IoT Goes Nuclear: Creating a ZigBee Chain Reaction. , 2017, , .		274
12	Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. , 2016, , .		129
13	New Second-Preimage Attacks on Hash Functions. Journal of Cryptology, 2016, 29, 657-696.	2.1	18
14	Bug Attacks. Journal of Cryptology, 2016, 29, 775-805.	2.1	6
15	Key Recovery Attacks on Iterated Evenâ€“Mansour Encryption Schemes. Journal of Cryptology, 2016, 29, 697-728.	2.1	14
16	Reflections on slide with a twist attacks. Designs, Codes, and Cryptography, 2015, 77, 633-651.	1.0	3
17	Improved Single-Key Attacks on 8-Round AES-192 and AES-256. Journal of Cryptology, 2015, 28, 397-422.	2.1	24
18	Slidex Attacks on the Evenâ€“Mansour Encryption Scheme. Journal of Cryptology, 2015, 28, 1-28.	2.1	22

#	Article	IF	Citations
19	New Attacks on IDEA with at Least 6 Rounds. Journal of Cryptology, 2015, 28, 209-239.	2.1	9
20	Almost universal forgery attacks on AES-based MACâ€™s. Designs, Codes, and Cryptography, 2015, 76, 431-449.	1.0	4
21	Improved Top-Down Techniques in Differential Cryptanalysis. Lecture Notes in Computer Science, 2015, , 139-156.	1.0	5
22	Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64. Lecture Notes in Computer Science, 2015, , 390-410.	1.0	1
23	Dissection. Communications of the ACM, 2014, 57, 98-105.	3.3	2
24	Improved Practical Attacks on Round-Reduced Keccak. Journal of Cryptology, 2014, 27, 183-209.	2.1	21
25	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	40
26	RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Lecture Notes in Computer Science, 2014, , 444-461.	1.0	182
27	Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. Lecture Notes in Computer Science, 2014, , 439-457.	1.0	17
28	Key Recovery Attacks on 3-round Even-Mansour, 8-step LED-128, and Full AES2. Lecture Notes in Computer Science, 2013, , 337-356.	1.0	29
29	Efficient Dissection of Composite Problems, with Applications to Cryptanalysis, Knapsacks, and Combinatorial Search Problems. Lecture Notes in Computer Science, 2012, , 719-740.	1.0	50
30	Applying cube attacks to stream ciphers in realistic scenarios. Cryptography and Communications, 2012, 4, 217-232.	0.9	22
31	Improved Attacks on Full GOST. Lecture Notes in Computer Science, 2012, , 9-28.	1.0	42
32	Minimalism in Cryptography: The Even-Mansour Scheme Revisited. Lecture Notes in Computer Science, 2012, , 336-354.	1.0	97
33	RFID Authentication Efficient Proactive Information Security withinÂComputational Security. Theory of Computing Systems, 2011, 48, 132-149.	0.7	10
34	Efficient Cache Attacks on AES, and Countermeasures. Journal of Cryptology, 2010, 23, 37-71.	2.1	325
35	Structural Cryptanalysis of SASAS. Journal of Cryptology, 2010, 23, 505-518.	2.1	41
36	Generic Analysis of Small Cryptographic Leaks. , 2010, , .		4

#	Article	IF	Citations
37	Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. Lecture Notes in Computer Science, 2010, , 299-319.	1.0	85
38	Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium. Lecture Notes in Computer Science, 2009, , 1-22.	1.0	107
39	Cube Attacks on Tweakable Black Box Polynomials. Lecture Notes in Computer Science, 2009, , 278-299.	1.0	240
40	Improved Related-key Attacks on DESX and DESX+. Cryptologia, 2008, 32, 13-22.	0.4	3
41	Second Preimage Attacks on Dithered Hash Functions. , 2008, , 270-288.		44
42	Length-based cryptanalysis: the case of Thompson's group. Journal of Mathematical Cryptology, 2007, 1, .	0.4	7
43	Remote Password Extraction from RFID Tags. IEEE Transactions on Computers, 2007, 56, 1292-1296.	2.4	56
44	Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Journal of Cryptology, 2005, 18, 291-311.	2.1	95
45	The LSD Broadcast Encryption Scheme. Lecture Notes in Computer Science, 2002, , 47-60.	1.0	259
46	Real Time Cryptanalysis of A5/1 on a PC. Lecture Notes in Computer Science, 2001, , 1-18.	1.0	239
47	Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. Lecture Notes in Computer Science, 2000, , 1-13.	1.0	201
48	Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. Lecture Notes in Computer Science, 2000, , 392-407.	1.0	383
49	Miss in the Middle Attacks on IDEA and Khufu. Lecture Notes in Computer Science, 1999, , 124-138.	1.0	103
50	Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. Lecture Notes in Computer Science, 1999, , 362-375.	1.0	34
51	Differential Cryptanalysis of the Data Encryption Standard. , 1993, , .		623
52	Differential Cryptanalysis of the Full 16-round DES. , 1992, , 487-496.		133
53	Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4, 3-72.	2.1	1,702
54	Differential Cryptanalysis of Feal and N-Hash. , 1991, , 1-16.		34

#	Article	IF	Citations
55	Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. , 1991, , 156-171.		45
56	How to find a battleship. Networks, 1989, 19, 361-371.	1.6	12
57	Efficient Factoring Based on Partial Information. , 1985, , 31-34.		46
58	On the generation of cryptographically strong pseudorandom sequences. ACM Transactions on Computer Systems, 1983, 1, 38-44.	0.6	180
59	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.	0.8	159
60	How to share a secret. Communications of the ACM, 1979, 22, 612-613.	3.3	10,025
61	The convergence of functions to fixedpoints of recursive definitions. Theoretical Computer Science, 1978, 6, 109-141.	0.5	14
62	A New Approach to Recursive Programs. , 1977, , 103-124.		1
63	The Theoretical Aspects of the Optimal Fixedpoint. SIAM Journal on Computing, 1976, 5, 414-426.	0.8	31