Orr Dunkelman

List of Publications by Year in Descending Order

80 papers	1,548 citations	22 h-index	36 g-index
80 ext. papers	1,742 ext. citations	1.3 avg, IF	4.72 L-index

#	Paper	IF	Citations
80	Practical key recovery attacks on FlexAEAD. *Designs, Codes, and Cryptography*, **2022**, 90, 983-1007	1.2	
79	Collaboration between Government and Research Community to Respond to COVID-19: Israel's Case. *Journal of Open Innovation: Technology, Market, and Complexity*, **2021**, 7, 208	3.7	0
78	Biased differential distinguisher Cryptanalysis of reduced-round SKINNY. *Information and Computation*, **2021**, 281, 104796	0.8	1
77	Inverting Binarizations of Facial Templates Produced by Deep Learning (and Its Implications). *IEEE Transactions on Information Forensics and Security*, **2021**, 16, 4184-4196	8	1
76	Single Tweakey Cryptanalysis of Reduced-Round SKINNY-64. *Lecture Notes in Computer Science*, **2020**, 1-17	0.9	1
75	Counting Active S-Boxes is not Enough. *Lecture Notes in Computer Science*, **2020**, 332-344	0.9	
74	Tight Bounds on Online Checkpointing Algorithms. *ACM Transactions on Algorithms*, **2020**, 16, 1-22	1.2	
73	New Slide Attacks on Almost Self-similar Ciphers. *Lecture Notes in Computer Science*, **2020**, 250-279	0.9	2
72	The Retracing Boomerang Attack. *Lecture Notes in Computer Science*, **2020**, 280-309	0.9	8
71	A Practical Forgery Attack on Lilliput-AE. *Journal of Cryptology*, **2020**, 33, 910-916	2.1	2
70	Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities. *Journal of Cryptology*, **2020**, 33, 1003-1043	2.1	5
69	DLCT: A New Tool for Differential-Linear Cryptanalysis. *Lecture Notes in Computer Science*, **2019**, 313-342	0.9	18
68	Linear Cryptanalysis Reduced Round of Piccolo-80. *Lecture Notes in Computer Science*, **2019**, 16-32	0.9	1
67	Efficient Dissection of Bicomposite Problems with Cryptanalytic Applications. *Journal of Cryptology*, **2019**, 32, 1448-1490	2.1	2
66	It is All in the System's Parameters: Privacy and Security Issues in Transforming Biometric Raw Data into Binary Strings. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 16, 796-804	3.9	4
65	Efficient Construction of the Kite Generator Revisited. *Lecture Notes in Computer Science*, **2018**, 6-19	0.9	
64	Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities. *Lecture Notes in Computer Science*, **2018**, 185-212	0.9	9

63	Efficient Slide Attacks. *Journal of Cryptology*, **2018**, 31, 641-670	2.1	12
62	WEM: A New Family of White-Box Block Ciphers Based on the Even-Mansour Construction. *Lecture Notes in Computer Science*, **2017**, 293-308	0.9	11
61	No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 2640-2653	8	74
60	Efficient Construction of Diamond Structures. *Lecture Notes in Computer Science*, **2017**, 166-185	0.9	2
59	GenFace: Improving Cyber Security Using Realistic Synthetic Face Generation. *Lecture Notes in Computer Science*, **2017**, 19-33	0.9	3
58	New Second Preimage Attacks on Dithered Hash Functions with Low Memory Complexity. *Lecture Notes in Computer Science*, **2017**, 247-263	0.9	1
57	Key Recovery Attacks on Iterated Even-Mansour Encryption Schemes. *Journal of Cryptology*, **2016**, 29, 697-728	2.1	10
56	New Second-Preimage Attacks on Hash Functions. *Journal of Cryptology*, **2016**, 29, 657-696	2.1	15
55	Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *Journal of Cryptology*, **2015**, 28, 397-422	2.1	17
54	Slidex Attacks on the Even-Mansour Encryption Scheme. *Journal of Cryptology*, **2015**, 28, 1-28	2.1	15
53	New Attacks on IDEA with at Least 6 Rounds. *Journal of Cryptology*, **2015**, 28, 209-239	2.1	8
52	Almost universal forgery attacks on AES-based MAC. *Designs, Codes, and Cryptography*, **2015**, 76, 431-449	1.2	4
51	Practical-time attacks against reduced variants of MISTY1. *Designs, Codes, and Cryptography*, **2015**, 76, 601-627	1.2	2
50	Reflections on slide with a twist attacks. *Designs, Codes, and Cryptography*, **2015**, 77, 633-651	1.2	3
49	Improved Top-Down Techniques in Differential Cryptanalysis. *Lecture Notes in Computer Science*, **2015**, 139-156	0.9	4
48	Cryptanalysis of SP Networks with Partial Non-Linear Layers. *Lecture Notes in Computer Science*, **2015**, 315-342	0.9	16
47	New Attacks on Feistel Structures with Improved Memory Complexities. *Lecture Notes in Computer Science*, **2015**, 433-454	0.9	16
46	Dissection. *Communications of the ACM*, **2014**, 57, 98-105	2.5	1

45	Improved Practical Attacks on Round-Reduced Keccak. *Journal of Cryptology*, **2014**, 27, 183-209	2.1	19
44	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
43	Cryptanalysis of Iterated Even-Mansour Schemes with Two Keys. *Lecture Notes in Computer Science*, **2014**, 439-457	0.9	13
42	Cryptanalysis of the Stream Cipher LEX. *Designs, Codes, and Cryptography*, **2013**, 67, 357-373	1.2	3
41	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
40	Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis. *IEEE Transactions on Information Theory*, **2012**, 58, 4948-4966	2.8	18
39	A Practical Attack on KeeLoq. *Journal of Cryptology*, **2012**, 25, 136-157	2.1	9
38	Low-Data Complexity Attacks on AES. *IEEE Transactions on Information Theory*, **2012**, 58, 7002-7017	2.8	30
37	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
36	Improved Attacks on Full GOST. *Lecture Notes in Computer Science*, **2012**, 9-28	0.9	32
35	New Insights on Impossible Differential Cryptanalysis. *Lecture Notes in Computer Science*, **2012**, 243-259	0.9	13
34	Minimalism in Cryptography: The Even-Mansour Scheme Revisited. *Lecture Notes in Computer Science*, **2012**, 336-354	0.9	82
33	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
32	A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *Lecture Notes in Computer Science*, **2010**, 393-410	0.9	60
31	Another Look at Complementation Properties. *Lecture Notes in Computer Science*, **2010**, 347-364	0.9	23
30	The effects of the omission of last round's MixColumns on AES. *Information Processing Letters*, **2010**, 110, 304-308	0.8	16
29	Cryptanalysis of CTC2. *Lecture Notes in Computer Science*, **2009**, 226-239	0.9	9
28	Cryptanalysis of Vortex. *Lecture Notes in Computer Science*, **2009**, 14-28	0.9	1

27	Cryptanalysis of Dynamic SHA(2). *Lecture Notes in Computer Science*, **2009**, 415-432	0.9	1
26	New Impossible Differential Attacks on AES. *Lecture Notes in Computer Science*, **2008**, 279-293	0.9	59
25	Treatment of the initial value in Time-Memory-Data Tradeoff attacks on stream ciphers. *Information Processing Letters*, **2008**, 107, 133-137	0.8	20
24	A Unified Approach to Related-Key Attacks. *Lecture Notes in Computer Science*, **2008**, 73-96	0.9	19
23	Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. *Lecture Notes in Computer Science*, **2008**, 370-386	0.9	50
22	An Improved Impossible Differential Attack on MISTY1. *Lecture Notes in Computer Science*, **2008**, 441-454	0.9	22
21	A New Attack on the LEX Stream Cipher. *Lecture Notes in Computer Science*, **2008**, 539-556	0.9	14
20	A Differential-Linear Attack on 12-Round Serpent. *Lecture Notes in Computer Science*, **2008**, 308-321	0.9	23
19	Improved Slide Attacks. *Lecture Notes in Computer Science*, **2007**, 153-166	0.9	16
18	A New Criterion for Nonlinearity of Block Ciphers. *IEEE Transactions on Information Theory*, **2007**, 53, 3944-3957	2.8	3
17	A New Attack on 6-Round IDEA. *Lecture Notes in Computer Science*, **2007**, 211-224	0.9	16
16	Improved Meet-in-the-Middle Attacks on Reduced-Round DES **2007**, 86-100		21
15	The Delicate Issues of Addition with Respect to XOR Differences. *Lecture Notes in Computer Science* , **2007**, 212-231	0.9	11
14	New Cryptanalytic Results on IDEA. *Lecture Notes in Computer Science*, **2006**, 412-427	0.9	16
13	A Simple Related-Key Attack on the Full SHACAL-1. *Lecture Notes in Computer Science*, **2006**, 20-30	0.9	5
12	New Combined Attacks on Block Ciphers. *Lecture Notes in Computer Science*, **2005**, 126-144	0.9	12
11	A Related-Key Rectangle Attack on the Full KASUMI. *Lecture Notes in Computer Science*, **2005**, 443-461	0.9	51
10	Related-Key Boomerang and Rectangle Attacks. *Lecture Notes in Computer Science*, **2005**, 507-525	0.9	99

9	Differential-Linear Cryptanalysis of Serpent. *Lecture Notes in Computer Science*, **2003**, 9-21	0.9	23
8	Enhancing Differential-Linear Cryptanalysis. *Lecture Notes in Computer Science*, **2002**, 254-266	0.9	43
7	Linear Cryptanalysis of Reduced Round Serpent. *Lecture Notes in Computer Science*, **2002**, 16-27	0.9	23
6	New Results on Boomerang and Rectangle Attacks. *Lecture Notes in Computer Science*, **2002**, 1-16	0.9	53
5	Differential and Linear Cryptanalysis of a Reduced-Round SC2000. *Lecture Notes in Computer Science*, **2002**, 34-48	0.9	4
4	The Rectangle Attack Rectangling the Serpent. *Lecture Notes in Computer Science*, **2001**, 340-357	0.9	123
3	Cryptanalysis of the A5/1 GSM Stream Cipher. *Lecture Notes in Computer Science*, **2000**, 43-51	0.9	42
2	Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. *Lecture Notes in Computer Science*, **1999**, 362-375	0.9	22
1	Cryptanalysis of GOST2. *IACR Transactions on Symmetric Cryptology*,203-214		2