Alex Biryukov

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/7853199/publications.pdf

Version: 2024-02-01

91 papers	4,407 citations	159525 30 h-index	138417 58 g-index
97 all docs	97 docs citations	97 times ranked	1564 citing authors

#	Article	IF	Citations
1	Dummy Shuffling Against Algebraic Attacks in White-Box Implementations. Lecture Notes in Computer Science, 2021, , 219-248.	1.0	5
2	On degree-d zero-sum sets of full rank. Cryptography and Communications, 2020, 12, 685-710.	0.9	2
3	ReCon: Sybil-resistant consensus from reputation. Pervasive and Mobile Computing, 2020, 61, 101109.	2.1	20
4	Alzette: A 64-Bit ARX-box. Lecture Notes in Computer Science, 2020, , 419-448.	1.0	22
5	FELICS-AEAD: Benchmarking of Lightweight Authenticated Encryption Algorithms. Lecture Notes in Computer Science, 2020, , 216-233.	1.0	8
6	Triathlon of lightweight block ciphers for the Internet of things. Journal of Cryptographic Engineering, 2019, 9, 283-302.	1.5	60
7	Privacy and Linkability of Mining in Zcash. , 2019, , .		8
8	Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis. , 2019, , .		51
9	Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. Pervasive and Mobile Computing, 2019, 59, 101030.	2.1	37
10	Transaction Clustering Using Network Traffic Analysis for Bitcoin and Derived Blockchains. , 2019, , .		13
11	Privacy Aspects and Subliminal Channels in Zcash. , 2019, , .		14
12	Portrait of a Miner in a Landscape. , 2019, , .		3
13	Optimal First-Order Boolean Masking for Embedded IoT Devices. Lecture Notes in Computer Science, 2018, , 22-41.	1.0	9
14	Attacks and Countermeasures for White-box Designs. Lecture Notes in Computer Science, 2018, , 373-402.	1.0	18
15	Symmetrically and Asymmetrically Hard Cryptography. Lecture Notes in Computer Science, 2017, , 417-445.	1.0	6
16	Side-Channel Attacks Meet Secure Network Protocols. Lecture Notes in Computer Science, 2017, , 435-454.	1.0	7
17	Findel: Secure Derivative Contracts for Ethereum. Lecture Notes in Computer Science, 2017, , 453-467.	1.0	32
18	Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications. , 2016, , .		100

#	Article	IF	Citations
19	Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. , 2016, , .		18
20	Cryptanalysis of Feistel Networks with Secret Round Functions. Lecture Notes in Computer Science, 2016, , 102-121.	1.0	17
21	Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice. Lecture Notes in Computer Science, 2016, , 537-557.	1.0	17
22	Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1. Lecture Notes in Computer Science, 2016, , 372-402.	1.0	32
23	Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. Lecture Notes in Computer Science, 2016, , 289-310.	1.0	37
24	Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem. Lecture Notes in Computer Science, 2016, , 93-122.	1.0	25
25	Design Strategies for ARX with Provable Bounds: Sparx and LAX. Lecture Notes in Computer Science, 2016, , 484-513.	1.0	74
26	Differential Analysis and Meet-in-the-Middle Attack Against Round-Reduced TWINE. Lecture Notes in Computer Science, 2015, , 3-27.	1.0	24
27	Differential Analysis of Block Ciphers SIMON and SPECK. Lecture Notes in Computer Science, 2015, , 546-570.	1.0	83
28	On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure. Lecture Notes in Computer Science, 2015, , 116-140.	1.0	23
29	Bitcoin over Tor isn't a Good Idea. , 2015, , .		105
30	Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay. Lecture Notes in Computer Science, 2015, , 445-455.	1.0	14
31	Tradeoff Cryptanalysis of Memory-Hard Functions. Lecture Notes in Computer Science, 2015, , 633-657.	1.0	15
32	Deanonymisation of Clients in Bitcoin P2P Network. , 2014, , .		318
33	Content and Popularity Analysis of Tor Hidden Services. , 2014, , .		88
34	Differential entropy analysis of the IDEA block cipher. Journal of Computational and Applied Mathematics, 2014, 259, 561-570.	1.1	6
35	Automatic Search for Differential Trails in ARX Ciphers. Lecture Notes in Computer Science, 2014, , 227-250.	1.0	57
36	PAEQ: Parallelizable Permutation-Based Authenticated Encryption. Lecture Notes in Computer Science, 2014, , 72-89.	1.0	19

#	Article	IF	Citations
37	Complementing Feistel Ciphers. Lecture Notes in Computer Science, 2014, , 3-18.	1.0	8
38	Cryptographic Schemes Based on the ASASA Structure:ÂBlack-Box,ÂWhite-Box, andÂPublic-Key (Extended) Tj ETQq0 0 0 rgBT /Overlock	1.0	63
39	Colliding Keys for SC2000-256. Lecture Notes in Computer Science, 2014, , 77-91.	1.0	0
40	Cryptanalysis of the Full AES Using GPU-Like Special-Purpose Hardware. Fundamenta Informaticae, 2012, 114, 221-237.	0.3	14
41	Differential Resynchronization Attacks on Reduced Round SNOW 3Gâ€‰âŠ•. Communications in Computer and Information Science, 2012, , 147-157.	0.4	4
42	TorScan: Tracing Long-Lived Connections and Differential Scanning Attacks. Lecture Notes in Computer Science, 2012, , 469-486.	1.0	7
43	Second-Order Differential Collisions for Reduced SHA-256. Lecture Notes in Computer Science, 2011, , 270-287.	1.0	41
44	Chosen Plaintext Attack. , 2011, , 205-206.		3
45	Related Key Attack. , 2011, , 1040-1041.		0
46	Slide Attack. , 2011, , 1221-1222.		0
47	Ciphertext-Only Attack. , 2011, , 207-207.		2
48	Data Encryption Standard (DES). , 2011, , 295-301.		117
49	Cryptanalysis of the Atmel Cipher in SecureMemory, CryptoMemory and CryptoRF. Lecture Notes in Computer Science, 2011, , 91-109.	1.0	7
50	Boomerang Attacks on BLAKE-32. Lecture Notes in Computer Science, 2011, , 218-237.	1.0	30
51	Search for Related-Key Differential Characteristics in DES-Like Ciphers. Lecture Notes in Computer Science, 2011, , 18-34.	1.0	13
52	Miss-in-the-Middle Attack. , 2011, , 786-786.		0
53	Skipjack. , 2011, , 1220-1221.		0
54	Impossible Differential Attack. , 2011, , 597-597.		8

#	Article	IF	Citations
55	Structural Cryptanalysis of SASAS. Journal of Cryptology, 2010, 23, 505-518.	2.1	41
56	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
57	Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and Others. Lecture Notes in Computer Science, 2010, , 322-344.	1.0	64
58	Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3Gâ€‰âŠ•. Lecture Notes in Computer Science, 2010, , 139-153.	1.0	13
59	Related-Key Cryptanalysis of the Full AES-192 and AES-256. Lecture Notes in Computer Science, 2009, , 1-18.	1.0	239
60	Speeding up Collision Search for Byte-Oriented Hash Functions. Lecture Notes in Computer Science, 2009, , 164-181.	1.0	18
61	Distinguisher and Related-Key Attack on the Full AES-256. Lecture Notes in Computer Science, 2009, , 231-249.	1.0	185
62	Design of a New Stream Cipherâ€"LEX. Lecture Notes in Computer Science, 2008, , 48-56.	1.0	7
63	Collisions for Step-Reduced SHA-256. Lecture Notes in Computer Science, 2008, , 1-15.	1.0	22
64	Slid Pairs in Salsa20 and Trivium. Lecture Notes in Computer Science, 2008, , 1-14.	1.0	14
65	Two New Techniques of Side-Channel Cryptanalysis. Lecture Notes in Computer Science, 2007, , 195-208.	1.0	21
66	Two Trivial Attacks on Trivium. , 2007, , 36-55.		51
67	Analysis of a SHA-256 Variant. Lecture Notes in Computer Science, 2006, , 245-260.	1.0	18
68	On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract). Lecture Notes in Computer Science, 2006, , 242-256.	1.0	63
69	The Design of a Stream Cipher LEX. Lecture Notes in Computer Science, 2006, , 67-75.	1.0	21
70	Analysis of the Non-linear Part of Mugi. Lecture Notes in Computer Science, 2005, , 320-329.	1.0	5
71	Recent attacks on alleged SecurID and their practical implications. Computers and Security, 2005, 24, 364-370.	4.0	8
72	Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Journal of Cryptology, 2005, 18, 291-311.	2.1	95

#	Article	IF	Citations
73	Non-randomness of the Full 4 and 5-Pass HAVAL. Lecture Notes in Computer Science, 2005, , 324-336.	1.0	7
74	A Distinguishing Attack of SNOWÂ2.0 with Linear Masking Method. Lecture Notes in Computer Science, 2004, , 222-233.	1.0	29
75	Cryptanalysis of Safer++. Lecture Notes in Computer Science, 2003, , 195-211.	1.0	30
76	A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. Lecture Notes in Computer Science, 2003, , 33-50.	1.0	87
77	Analysis of Involutional Ciphers: Khazad and Anubis. Lecture Notes in Computer Science, 2003, , 45-53.	1.0	30
78	Cryptanalysis of 3-Pass HAVAL. Lecture Notes in Computer Science, 2003, , 228-245.	1.0	19
79	New Weak-Key Classes of IDEA. Lecture Notes in Computer Science, 2002, , 315-326.	1.0	40
80	Real Time Cryptanalysis of A5/1 on a PC. Lecture Notes in Computer Science, 2001, , 1-18.	1.0	239
81	Structural Cryptanalysis of SASAS. Lecture Notes in Computer Science, 2001, , 395-405.	1.0	77
82	Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. Lecture Notes in Computer Science, 2000, , 1-13.	1.0	201
83	Advanced Slide Attacks. Lecture Notes in Computer Science, 2000, , 589-606.	1.0	141
84	Miss in the Middle Attacks on IDEA and Khufu. Lecture Notes in Computer Science, 1999, , 124-138.	1.0	103
85	Initial Observations on Skipjack: Cryptanalysis of Skipjack-3XOR. Lecture Notes in Computer Science, 1999, , 362-375.	1.0	34
86	Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Lecture Notes in Computer Science, 1999, , 12-23.	1.0	331
87	From differential cryptanalysis to ciphertext-only attacks. Lecture Notes in Computer Science, 1998, , 72-88.	1.0	22
88	Improved cryptanalysis of RC5. Lecture Notes in Computer Science, 1998, , 85-99.	1.0	51
89	An improvement of Daviesâ€™ attack on DES. Journal of Cryptology, 1997, 10, 195-205.	2.1	31
90	How to strengthen DES using existing hardware. Lecture Notes in Computer Science, 1995, , 398-412.	1.0	23

#	Article	IF	Citations
91	Multiset-Algebraic Cryptanalysis of Reduced Kuznyechik, Khazad, and secret SPNs. IACR Transactions on Symmetric Cryptology, 0, , 226-247.	0.0	7