Christoph Dobraunig

List of Publications by Year
in descending order

35	629	687363 13	713466 21
papers	citations	h-index	g-index

37	37	37	279
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 547-572.	0.0	96
2	Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology, 2021, 34, 1.	2.8	68
3	Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. Lecture Notes in Computer Science, 2018, , 662-692.	1.3	46
4	Statistical Ineffective Fault Attacks onÂMasked AES with Fault Countermeasures. Lecture Notes in Computer Science, 2018, , 315-342.	1.3	42
5	ISAP â€“ Towards Side-Channel Secure Authenticated Encryption. IACR Transactions on Symmetric Cryptology, 0, , 80-105.	0.0	36
6	Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes. Lecture Notes in Computer Science, 2016, , 369-395.	1.3	35
7	Analysis of SHA-512/224 and SHA-512/256. Lecture Notes in Computer Science, 2015, , 612-630.	1.3	32
8	Isap v2.0. IACR Transactions on Symmetric Cryptology, 0, , 390-416.	0.0	26
9	Suit up! -- Made-to-Measure Hardware Implementations of ASCON. , 2015, , .		24
10	Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security. Lecture Notes in Computer Science, 2016, , 225-241.	1.3	23
11	Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. Lecture Notes in Computer Science, 2021, , 3-34.	1.3	21
12	Higher-Order Cryptanalysis of LowMC. Lecture Notes in Computer Science, 2016, , 87-101.	1.3	20
13	Ascon hardware implementations and side-channel evaluation. Microprocessors and Microsystems, 2017, 52, 470-479.	2.8	19
14	Leakage Resilience of the Duplex Construction. Lecture Notes in Computer Science, 2019, , 225-255.	1.3	15
15	Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates. Lecture Notes in Computer Science, 2015, , 490-509.	1.3	14
16	Square Attack on 7-Round Kiasu-BC. Lecture Notes in Computer Science, 2016, , 500-517.	1.3	13
17	Differential Cryptanalysis of SipHash. Lecture Notes in Computer Science, 2014, , 165-182.	1.3	9
18	Impossible-Differential and Boomerang Cryptanalysis of Round-Reduced Kiasu-BC. Lecture Notes in Computer Science, 2017, , 207-222.	1.3	8

#	Article	IF	Citations
19	Fault Attacks on Nonce-Based Authenticated Encryption: Application to Keyak and Ketje. Lecture Notes in Computer Science, 2019, , 257-277.	1.3	7
20	On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks. Lecture Notes in Computer Science, 2015, , 233-244.	1.3	6
21	Compact Hardware Implementations of the Block Ciphers mCrypton, NOEKEON, and SEA. Lecture Notes in Computer Science, 2012, , 358-377.	1.3	6
22	Leakage Resilient Value Comparison with Application to Message Authentication. Lecture Notes in Computer Science, 2021, , 377-407.	1.3	5
23	Related-Key Forgeries for PrÃ¸st-OTR. Lecture Notes in Computer Science, 2015, , 282-296.	1.3	5
24	Framework for faster key search using relatedâ€key higherâ€order differentialproperties: applications to Agrasta. IET Information Security, 2020, 14, 202-209.	1.7	4
25	Efficient Collision Attack Frameworks for RIPEMD-160. Lecture Notes in Computer Science, 2019, , 117-149.	1.3	4
26	Analysis of the Kupyna-256 Hash Function. Lecture Notes in Computer Science, 2016, , 575-590.	1.3	3
27	Multi-user Security of the Elephant v2 Authenticated Encryption Mode. Lecture Notes in Computer Science, 2022, , 155-178.	1.3	3
28	Information-Combining Differential Fault Attacks onÂDEFAULT. Lecture Notes in Computer Science, 2022, , 168-191.	1.3	3
29	Side-Channel Analysis of Keymill. Lecture Notes in Computer Science, 2017, , 138-152.	1.3	2
30	Forgery Attacks on Round-Reduced ICEPOLE-128. Lecture Notes in Computer Science, 2016, , 479-492.	1.3	2
31	Algebraic Cryptanalysis of Variants of Frit. Lecture Notes in Computer Science, 2020, , 149-170.	1.3	2
32	Improved (semi-free-start/near-) collision and distinguishing attacks on round-reduced RIPEMD-160. Designs, Codes, and Cryptography, 2020, 88, 887-930.	1.6	1
33	Cryptanalysis of Simpira v1. Lecture Notes in Computer Science, 2017, , 284-298.	1.3	1
34	Tightness of the Suffix Keyed Sponge Bound. IACR Transactions on Symmetric Cryptology, 0, , 195-212.	0.0	1
35	Practical forgeries for ORANGE. Information Processing Letters, 2020, 159-160, 105961.	0.6	0