Martin Hell

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/5121628/publications.pdf

Version: 2024-02-01

40

papers

1,033

citations

933447

10

h-index

526287

27

g-index

41

all docs

41

docs citations

41

times ranked

482

citing authors

#	Article	IF	Citations
1	Grain: a stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, 2007, 2, 86.	0.2	285
2	A Stream Cipher Proposal: Grain-128. , 2006, , .		165
3	Grain-128a: a new version of Grain-128 with optional authentication. International Journal of Wireless and Mobile Computing, 2011, 5, 48.	0.2	152
4	The Grain Family of Stream Ciphers. Lecture Notes in Computer Science, 2008, , 179-190.	1.3	149
5	Espresso: A stream cipher for 5G wireless communication systems. Cryptography and Communications, 2017, 9, 273-289.	1.4	40
6	Towards a General RC4-Like Keystream Generator. Lecture Notes in Computer Science, 2005, , 162-174.	1.3	36
7	An overview of distinguishing attacks on stream ciphers. Cryptography and Communications, 2009, 1, 71-94.	1.4	25
8	Breaking the F-FCSR-H Stream Cipher in Real Time. Lecture Notes in Computer Science, 2008, , 557-569.	1.3	24
9	Blockchain-Based Publishing Layer for the Keyless Signing Infrastructure. , 2016, , .		15
10	Breaking the Stream Ciphers F-FCSR-H and F-FCSR-16 in Real Time. Journal of Cryptology, 2011, 24, 427-445.	2.8	14
11	A Note on Distinguishing Attacks. , 2007, , .		12
12	Improved distinguishers for HC-128. Designs, Codes, and Cryptography, 2012, 63, 225-240.	1.6	12
13	On Hardware-Oriented Message Authentication with Applications towards RFID. , 2011, , .		11
14	A survey on fast correlation attacks. Cryptography and Communications, 2012, 4, 173-202.	1.4	11
15	An AEAD Variant of the Grain Stream Cipher. Lecture Notes in Computer Science, 2019, , 55-71.	1.3	10
16	A new instruction overlapping technique for anti-disassembly and obfuscation of x86 binaries. , 2013, , .		9
17	Visual Cryptography and Obfuscation: A Use-Case for Decrypting and Deobfuscating Information Using Augmented Reality. Lecture Notes in Computer Science, 2015, , 261-273.	1.3	9
18	Efficient Hardware Implementations of Grain-128AEAD. Lecture Notes in Computer Science, 2019, , 495-513.	1.3	7

#	Article	IF	Citations
19	An Efficient State Recovery Attack on X-FCSR-256. Lecture Notes in Computer Science, 2009, , 23-37.	1.3	6
20	Correlation Attacks Using aÂNew Class of Weak Feedback Polynomials. Lecture Notes in Computer Science, 2004, , 127-142.	1.3	5
21	Improved Greedy Nonrandomness Detectors for Stream Ciphers. , 2017, , .		5
22	Improved Distinguishers on Stream Ciphers With Certain Weak Feedback Polynomials. IEEE Transactions on Information Theory, 2012, 58, 6183-6193.	2.4	4
23	An Efficient State Recovery Attack on the X-FCSR Family of Stream Ciphers. Journal of Cryptology, 2014, 27, 1-22.	2.8	4
24	Grain-128AEADv2: Strengthening theÂInitialization Against Key Reconstruction. Lecture Notes in Computer Science, 2021, , 24-41.	1.3	3
25	Cryptanalysis of the stream cipher BEAN. , 2011, , .		2
26	Improved message passing techniques in fast correlation attacks on stream ciphers. , 2012, , .		2
27	A Technique for Remote Detection of Certain Virtual Machine Monitors. Lecture Notes in Computer Science, 2012, , 129-137.	1.3	2
28	Exploiting Trust in Deterministic Builds. Lecture Notes in Computer Science, 2016, , 238-249.	1.3	2
29	eavesROP: Listening for ROP Payloads in Data Streams. Lecture Notes in Computer Science, 2014, , 413-424.	1.3	2
30	Not So Greedy: Enhanced Subset Exploration for Nonrandomness Detectors. Communications in Computer and Information Science, 2018, , 273-294.	0.5	2
31	Another look at weak feedback polynomials in the nonlinear combiner. , 2009, , .		1
32	Searching for New Convolutional Codes using the Cell Broadband Engine Architecture. IEEE Communications Letters, 2011, 15, 560-562.	4.1	1
33	An optimal sampling technique for distinguishing random S-boxes. , 2012, , .		1
34	Improved Key Recovery Attack on the BEAN Stream Cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 1437-1444.	0.3	1
35	Analysis of Xorrotation with Application to an HC-128 Variant. Lecture Notes in Computer Science, 2012, , 419-425.	1.3	1
36	Enabling Key Migration Between Non-compatible TPM Versions. Lecture Notes in Computer Science, 2016, , 101-118.	1.3	1

#	Article	IF	Citations
37	Using coding techniques to analyze weak feedback polynomials. , 2010, , .		0
38	The efficiency of optimal sampling in the random S-box model. , 2014, , .		0
39	Improving the Rainbow Attack by Reusing Colours. Lecture Notes in Computer Science, 2009, , 362-378.	1.3	0
40	Using TPM Secure Storage in Trusted High Availability Systems. Lecture Notes in Computer Science, 2015, , 243-258.	1.3	0