Thomas Peyrin

List of Publications by Year
in descending order

57 papers	2,634 citations	318942 23 h-index	214428 50 g-index
61 all docs	61 docs citations	61 times ranked	796 citing authors

#	Article	IF	Citations
1	The Deoxys AEAD Family. Journal of Cryptology, 2021, 34, 1.	2.1	9
2	DEFAULT: Cipher Level Resistance Against Differential Fault Attack. Lecture Notes in Computer Science, 2021, , 124-156.	1.0	12
3	The MALICIOUS Framework: Embedding Backdoors into Tweakable Block Ciphers. Lecture Notes in Computer Science, 2020, , 249-278.	1.0	14
4	NeuroGIFT: Using a Machine Learning Based Sat Solver for Cryptanalysis. Lecture Notes in Computer Science, 2020, , 62-84.	1.0	2
5	SoK. , 2019, , .		2
6	From Collisions to Chosen-Prefix Collisions Application to Full SHA-1. Lecture Notes in Computer Science, 2019, , 527-555.	1.0	20
7	Crack me if you can: hardware acceleration bridging the gap between practical and theoretical cryptanalysis?. , 2018, , .		1
8	Boomerang Connectivity Table: A New Cryptanalysis Tool. Lecture Notes in Computer Science, 2018, , 683-714.	1.0	72
9	Protecting block ciphers against differential fault attacks without re-keying. , 2018, , .		16
10	ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. Lecture Notes in Computer Science, 2017, , 34-65.	1.0	33
11	GIFT: A Small Present. Lecture Notes in Computer Science, 2017, , 321-345.	1.0	221
12	Bit-Sliding: A Generic Technique for Bit-Serial Implementations of SPN-based Primitives. Lecture Notes in Computer Science, 2017, , 687-707.	1.0	28
13	Looting the LUTs: FPGA Optimization of AES and AES-like Ciphers for Authenticated Encryption. Lecture Notes in Computer Science, 2017, , 282-301.	1.0	11
14	Freestart Collision for Full SHA-1. Lecture Notes in Computer Science, 2016, , 459-483.	1.0	28
15	The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. Lecture Notes in Computer Science, 2016, , 123-153.	1.0	310
16	Cryptanalysis of Full RIPEMD-128. Journal of Cryptology, 2016, 29, 927-951.	2.1	1
17	Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. Lecture Notes in Computer Science, 2016, , 33-63.	1.0	64
18	Practical Free-Start Collision Attacks on 76-step SHA-1. Lecture Notes in Computer Science, 2015, , 623-642.	1.0	20

#	Article	IF	Citations
19	Collision Attack on Grindahl. Journal of Cryptology, 2015, 28, 879-898.	2.1	1
20	Known-Key Distinguisher on Full PRESENT. Lecture Notes in Computer Science, 2015, , 455-474.	1.0	12
21	Cryptanalysis of JAMBU. Lecture Notes in Computer Science, 2015, , 264-281.	1.0	5
22	Lightweight MDS Involution Matrices. Lecture Notes in Computer Science, 2015, , 471-493.	1.0	44
23	Improved Cryptanalysis of AES-like Permutations. Journal of Cryptology, 2014, 27, 772-798.	2.1	6
24	A Very Compact FPGA Implementation of LED and PHOTON. Lecture Notes in Computer Science, 2014, , 304-321.	1.0	33
25	Generic Universal Forgery Attack on Iterative Hash-Based MACs. Lecture Notes in Computer Science, 2014, , 147-164.	1.0	17
26	Implementing Lightweight Block Ciphers on x86 Architectures. Lecture Notes in Computer Science, 2014, , 324-351.	1.0	17
27	Multiple Limited-Birthday Distinguishers and Applications. Lecture Notes in Computer Science, 2014, , 533-550.	1.0	15
28	Security Analysis of PRINCE. Lecture Notes in Computer Science, 2014, , 92-111.	1.0	27
29	Updates on Generic Attacks against HMAC and NMAC. Lecture Notes in Computer Science, 2014, , 131-148.	1.0	13
30	FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison. Lecture Notes in Computer Science, 2014, , 433-450.	1.0	36
31	Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. Lecture Notes in Computer Science, 2014, , 274-288.	1.0	121
32	Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128. Lecture Notes in Computer Science, 2013, , 183-203.	1.0	39
33	Cryptanalysis of Full RIPEMD-128. Lecture Notes in Computer Science, 2013, , 228-244.	1.0	11
34	New Generic Attacks against Hash-Based MACs. Lecture Notes in Computer Science, 2013, , 1-20.	1.0	21
35	Improved Cryptanalysis of Reduced RIPEMD-160. Lecture Notes in Computer Science, 2013, , 484-503.	1.0	12
36	Limited-Birthday Distinguishers for Hash Functions. Lecture Notes in Computer Science, 2013, , 504-523.	1.0	16

#	Article	IF	Citations
37	Unaligned Rebound Attack: Application to Keccak. Lecture Notes in Computer Science, 2012, , 402-421.	1.0	32
38	SPN-Hash: Improving the Provable Resistance against Differential Collision Attacks. Lecture Notes in Computer Science, 2012, , 270-286.	1.0	12
39	On the (In)Security of IDEA in Various Hashing Modes. Lecture Notes in Computer Science, 2012, , 163-179.	1.0	11
40	Improved Rebound Attack on the Finalist GrÃ¸stl. Lecture Notes in Computer Science, 2012, , 110-126.	1.0	25
41	Generic Related-Key Attacks for HMAC. Lecture Notes in Computer Science, 2012, , 580-597.	1.0	26
42	The LED Block Cipher. Lecture Notes in Computer Science, 2011, , 326-341.	1.0	481
43	The PHOTON Family of Lightweight Hash Functions. Lecture Notes in Computer Science, 2011, , 222-239.	1.0	306
44	Analysis of Reduced-SHAvite-3-256 v2. Lecture Notes in Computer Science, 2011, , 68-87.	1.0	3
45	Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations. Lecture Notes in Computer Science, 2010, , 365-383.	1.0	111
46	Cryptanalysis of the 10-Round Hash and Full Compression Function of SHAvite-3-512. Lecture Notes in Computer Science, 2010, , 419-436.	1.0	5
47	Improved Differential Attacks for ECHO and GrÃ¸stl. Lecture Notes in Computer Science, 2010, , 370-392.	1.0	46
48	Cryptanalysis of RadioGatÃºn. Lecture Notes in Computer Science, 2009, , 122-138.	1.0	3
49	Improved Cryptanalysis of the Reduced GrÃ¸stl Compression Function, ECHO Permutation and AES Block Cipher. Lecture Notes in Computer Science, 2009, , 16-35.	1.0	59
50	Collisions on SHA-0 in One Hour. Lecture Notes in Computer Science, 2008, , 16-35.	1.0	24
51	On Building Hash Functions from Multivariate Quadratic Equations. , 2007, , 82-95.		14
52	Hash Functions and the (Amplified) Boomerang Attack. , 2007, , 244-263.		45
53	Security Analysis of Constructions Combining FIL Random Oracles. Lecture Notes in Computer Science, 2007, , 119-136.	1.0	6
54	Cryptanalysis of Grindahl. Lecture Notes in Computer Science, 2007, , 551-567.	1.0	31

#	Article	IF	Citations
55	Combining Compression Functions and Block Cipher-Based Hash Functions. Lecture Notes in Computer Science, 2006, , 315-331.	1.0	21
56	Cryptanalysis of T-Function-Based Hash Functions. Lecture Notes in Computer Science, 2006, , 267-285.	1.0	3
57	A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers. IACR Transactions on Symmetric Cryptology, 0, , 73-107.	0.0	22