

MarÃ-a Naya-Plasencia

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11823158/publications.pdf>

Version: 2024-02-01

14
papers

310
citations

1040056

9
h-index

996975

15
g-index

15
all docs

15
docs citations

15
times ranked

98
citing authors

#	ARTICLE	IF	CITATIONS
1	Internal Symmetries and Linear Properties: Full-permutation Distinguishers and Improved Collisions on Gimli. <i>Journal of Cryptology</i> , 2021, 34, 1.	2.8	29
2	Improving Key-Recovery in Linear Attacks: Application to 28-Round PRESENT. <i>Lecture Notes in Computer Science</i> , 2020, , 221-249.	1.3	16
3	Cryptanalysis Results on Spook. <i>Lecture Notes in Computer Science</i> , 2020, , 359-388.	1.3	4
4	Making the Impossible Possible. <i>Journal of Cryptology</i> , 2018, 31, 101-133.	2.8	36
5	Improved Cryptanalysis of AES-like Permutations. <i>Journal of Cryptology</i> , 2014, 27, 772-798.	2.8	6
6	Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. <i>Lecture Notes in Computer Science</i> , 2014, , 179-199.	1.3	77
7	A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. <i>Information Processing Letters</i> , 2012, 112, 624-629.	0.6	27
8	Correlation attacks on combination generators. <i>Cryptography and Communications</i> , 2012, 4, 147-171.	1.4	4
9	Parity-Check Relations on Combination Generators. <i>IEEE Transactions on Information Theory</i> , 2012, 58, 3900-3911.	2.4	2
10	Improved Analysis of ECHO-256. <i>Lecture Notes in Computer Science</i> , 2012, , 19-36.	1.3	11
11	How to Improve Rebound Attacks. <i>Lecture Notes in Computer Science</i> , 2011, , 188-205.	1.3	32
12	Rebound Attack on the Full Lane Compression Function. <i>Lecture Notes in Computer Science</i> , 2009, , 106-125.	1.3	44
13	Cryptanalysis of Achterbahn-128/80. <i>Lecture Notes in Computer Science</i> , 2007, , 73-86.	1.3	10
14	Cryptanalysis of Achterbahn-128/80 with a New Keystream Limitation. <i>Lecture Notes in Computer Science</i> , 2007, , 142-152.	1.3	3