MarÃ-a Naya-Plasencia

List of Publications by Year
in descending order

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