Lorenzo Grassi

List of Publications by Year
in descending order

23	499	933447 10	839539 18
papers	citations	h-index	g-index

24	24	24	117
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity. Lecture Notes in Computer Science, 2016, , 191-219.	1.3	107
2	Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. Lecture Notes in Computer Science, 2018, , 662-692.	1.3	46
3	Feistel Structures for MPC, and More. Lecture Notes in Computer Science, 2019, , 151-171.	1.3	44
4	MPC-Friendly Symmetric Key Primitives. , 2016, , .		38
5	A New Structural-Differential Property of 5-Round AES. Lecture Notes in Computer Science, 2017, , 289-317.	1.3	38
6	Mixture Differential Cryptanalysis: a New Approach to Distinguishers and Attacks on round-reduced AES. IACR Transactions on Symmetric Cryptology, 0, , 133-160.	0.0	32
7	Algebraic Cryptanalysis ofÂSTARK-Friendly Designs: Application to MARVELlous and MiMC. Lecture Notes in Computer Science, 2019, , 371-397.	1.3	31
8	On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. Lecture Notes in Computer Science, 2020, , 674-704.	1.3	29
9	Ciminion: Symmetric Encryption Based on Toffoli-Gates over Large Finite Fields. Lecture Notes in Computer Science, 2021, , 3-34.	1.3	21
10	Subspace Trail Cryptanalysis and its Applications to AES. IACR Transactions on Symmetric Cryptology, 0, , 192-225.	0.0	21
11	Quantum Algorithms for the $$k$$-xor Problem. Lecture Notes in Computer Science, 2018, , 527-559.	1.3	17
12	An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC. Lecture Notes in Computer Science, 2020, , 477-506.	1.3	17
13	MixColumns Properties and Attacks on (Round-Reduced) AES with a Single Secret S-Box. Lecture Notes in Computer Science, 2018, , 243-263.	1.3	12
14	Zero-Sum Partitions of PHOTON Permutations. Lecture Notes in Computer Science, 2018, , 279-299.	1.3	11
15	Probabilistic Mixture Differential Cryptanalysis on Round-Reduced AES. Lecture Notes in Computer Science, 2020, , 53-84.	1.3	6
16	Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE. Lecture Notes in Computer Science, 2016, , 322-342.	1.3	5
17	Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box. Lecture Notes in Computer Science, 2020, , 312-331.	1.3	5
18	The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over Fnp. IACR Transactions on Symmetric Cryptology, 0, , 5-37.	0.0	5

#	Article	IF	Citations
19	Influence of the Linear Layer on the Algebraic Degree in SP-Networks. IACR Transactions on Symmetric Cryptology, 0, , 110-137.	0.0	4
20	Revisiting Gilbertâ€™s known-key distinguisher. Designs, Codes, and Cryptography, 2020, 88, 1401-1445.	1.6	3
21	Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer. IACR Transactions on Symmetric Cryptology, 0, , 314-352.	0.0	2
22	Algebraic Key-Recovery Attacks onÂReduced-Round Xoofff. Lecture Notes in Computer Science, 2021, , 171-197.	1.3	2
23	Simulations of Optical Emissions for Attacking AES and Masked AES. Lecture Notes in Computer Science, 2015, , 172-189.	1.3	2