Maria Isabel Gonzalez Vasco

List of Publications by Year
in descending order

39 papers	303 citations	1162367 8 h-index	996533 15 g-index
40 all docs	40 docs citations	40 times ranked	130 citing authors

#	Article	IF	Citations
1	Shuffle, Cut, and Learn: Crypto Go, a Card Game for Teaching Cryptography. Mathematics, 2020, 8, 1993.	1.1	6
2	Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber. Mathematics, 2020, 8, 1853.	1.1	4
3	Building Group Key Establishment on Group Theory: A Modular Approach. Symmetry, 2020, 12, 197.	1.1	2
4	Group Key Establishment in a Quantum-Future Scenario. Informatica, 2020, , 1-18.	1.5	3
5	The Cracking of WalnutDSA: A Survey. Symmetry, 2019, 11, 1072.	1.1	0
6	A key for John Doe: modeling and designing Anonymous Password-Authenticated Key Exchange protocols. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	4
7	Passwordâ€“Authenticated Group Key Establishment from Smooth Projective Hash Functions. International Journal of Applied Mathematics and Computer Science, 2019, 29, 797-815.	1.5	2
8	Group key exchange protocols withstanding ephemeralâ€key reveals. IET Information Security, 2018, 12, 79-86.	1.1	3
9	Analytic surveillance: Big data business models in the time of privacy awareness. Profesional De La Informacion, 2018, 27, 402.	2.7	5
10	The Roll of Dices in Cryptology. Studies in Systems, Decision and Control, 2018, , 493-504.	0.8	0
11	Partitioned Group Password-Based Authenticated Key Exchange. Computer Journal, 2017, 60, 1912-1922.	1.5	2
12	Private set intersection: New generic constructions and feasibility results. Advances in Mathematics of Communications, 2017, 11, 481-502.	0.4	1
13	Pitfalls in a server-aided authenticated group key establishment. Information Sciences, 2016, 363, 1-7.	4.0	1
14	Combined schemes for signature and encryption: The public-key and the identity-based setting. Information and Computation, 2016, 247, 1-10.	0.5	6
15	Cryptanalysis of a key exchange scheme based on block matrices. Information Sciences, 2014, 276, 319-331.	4.0	1
16	Flexible Anonymous Subscription Schemes. Communications in Computer and Information Science, 2012, , 203-219.	0.4	1
17	Size-Hiding in Private Set Intersection: Existential Results and Constructions. Lecture Notes in Computer Science, 2012, , 378-394.	1.0	9
18	A note on the security of MST 3. Designs, Codes, and Cryptography, 2010, 55, 189-200.	1.0	7

#	Article	IF	Citations
19	In search of mathematical primitives for deriving universal projective hash families. Applicable Algebra in Engineering, Communications and Computing, 2008, 19, 161-173.	0.3	1
20	Applications of algebra to cryptography. Discrete Applied Mathematics, 2008, 156, 3071.	0.5	0
21	Choosing a leader on a complex network. Journal of Computational and Applied Mathematics, 2007, 204, 10-17.	1.1	17
22	Secure group key establishment revisited. International Journal of Information Security, 2007, 6, 243-254.	2.3	62
23	Attacking a public key cryptosystem based on tree replacement. Discrete Applied Mathematics, 2007, 155, 61-67.	0.5	0
24	(Password) Authenticated Key Establishment: From 2-Party to Group. Lecture Notes in Computer Science, 2007, , 499-514.	1.0	25
25	Pitfalls in public key cryptosystems based on free partially commutative monoids and groups. Applied Mathematics Letters, 2006, 19, 1037-1041.	1.5	4
26	Entwurf asymmetrischer kryptographischer Verfahren unter BerÃ¼cksichtigung von Quantenalgorithmen (Design of Asymmetric Cryptographic Schemes Taking Into Account Quantum) Tj ETQq0 0 0 rgBT /Overlock 10 Tf	0	
27	A Subliminal-Free Variant of ECDSA. Lecture Notes in Computer Science, 2006, , 375-387.	1.0	7
28	Weak Keys in MST1. Designs, Codes, and Cryptography, 2005, 37, 509-524.	1.0	12
29	A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes. Lecture Notes in Computer Science, 2005, , 495-509.	1.0	8
30	On the Security of Two Public Key Cryptosystems Using Non-Abelian Groups. Designs, Codes, and Cryptography, 2004, 32, 207-216.	1.0	1
31	Towards a Uniform Description of Several Group Based Cryptographic Primitives. Designs, Codes, and Cryptography, 2004, 33, 215-226.	1.0	6
32	A Reaction Attack on a Public Key Cryptosystem Based on the Word Problem. Applicable Algebra in Engineering, Communications and Computing, 2004, 14, 335-340.	0.3	9
33	New Results on the Hardness of Diffie-HellmanÂBits. Lecture Notes in Computer Science, 2004, , 159-172.	1.0	8
34	On Minimal Length Factorizations of Finite Groups. Experimental Mathematics, 2003, 12, 1-12.	0.5	21
35	The Hidden Number Problem in Extension Fields and Its Applications. Lecture Notes in Computer Science, 2002, , 105-117.	1.0	4
36	Security of the most significant bits of the Shamir message passing scheme. Mathematics of Computation, 2001, 71, 333-343.	1.1	20

#	Article	IF	Citations
37	Clouds over a public key cryptosystem based on Lyndon words. Information Processing Letters, 2001, 80, 239-242.	0.4	3
38	A Survey of Hard Core Functions. , 2001, , 227-255.		11
39	On the Security of Diffie-Hellman Bits. , 2001, , 257-268.		27