Paulo S L M Barreto

List of Publications by Citations

Source: https://exaly.com/author-pdf/1836255/paulo-s-l-m-barreto-publications-by-citations.pdf
Version: 2024-04-28

64	2,643	21	51
papers	citations	h-index	g-index
68	2,917	1.4	5.11
ext. papers	ext. citations	avg, IF	L-index

#	Paper	IF	Citations
64	Efficient Algorithms for Pairing-Based Cryptosystems. *Lecture Notes in Computer Science*, **2002**, 354-369	0.9	407
63	Pairing-Friendly Elliptic Curves of Prime Order. *Lecture Notes in Computer Science*, **2006**, 319-331	0.9	382
62	Efficient pairing computation on supersingular Abelian varieties. *Designs, Codes, and Cryptography*, **2007**, 42, 239-271	1.2	229
61	Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. *Lecture Notes in Computer Science*, **2005**, 515-532	0.9	195
60	MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes **2013**,		170
59	A survey on key management mechanisms for distributed Wireless Sensor Networks. *Computer Networks*, **2010**, 54, 2591-2612	5.4	119
58	Efficient Implementation of Pairing-Based Cryptosystems. *Journal of Cryptology*, **2004**, 17, 321-334	2.1	90
57	Constructing Elliptic Curves with Prescribed Embedding Degrees. *Lecture Notes in Computer Science* , **2003**, 257-267	0.9	89
56	A New Two-Party Identity-Based Authenticated Key Agreement. *Lecture Notes in Computer Science*, **2005**, 262-274	0.9	83
55	Compact McEliece Keys from Goppa Codes. *Lecture Notes in Computer Science*, **2009**, 376-392	0.9	80
54	Toward secure public-key blockwise fragile authentication watermarking. *IET Computer Vision*, **2002** , 149, 57		69
53	On the Selection of Pairing-Friendly Groups. *Lecture Notes in Computer Science*, **2004**, 17-25	0.9	68
52	A family of implementation-friendly BN elliptic curves. *Journal of Systems and Software*, **2011**, 84, 1319-1326	3.3	60
51	Providing integrity and authenticity in DICOM images: a novel approach. *IEEE Transactions on Information Technology in Biomedicine*, **2009**, 13, 582-9		48
50	Compressed Pairings. *Lecture Notes in Computer Science*, **2004**, 140-156	0.9	46
49	Generating More MNT Elliptic Curves. *Designs, Codes, and Cryptography*, **2006**, 38, 209-217	1.2	41
48	Efficient Hardware for the Tate Pairing Calculation in Characteristic Three. *Lecture Notes in Computer Science*, **2005**, 412-426	0.9	41

47	Survey and comparison of message authentication solutions on wireless sensor networks. *Ad Hoc Networks*, **2013**, 11, 1221-1236	4.8	24
46	Rotation symmetry in algebraically generated cryptographic substitution tables. *Information Processing Letters*, **2008**, 106, 246-250	0.8	24
45	Whirlwind: a new cryptographic hash function. *Designs, Codes, and Cryptography*, **2010**, 56, 141-162	1.2	23
44	The MARVIN message authentication code and the LETTERSOUP authenticated encryption scheme. *Security and Communication Networks*, **2009**, 2, 165-180	1.9	22
43	One-time signature scheme from syndrome decoding over generic error-correcting codes. *Journal of Systems and Software*, **2011**, 84, 198-204	3.3	19
42	Subgroup Security in Pairing-Based Cryptography. *Lecture Notes in Computer Science*, **2015**, 245-265	0.9	19
41	Shorter hash-based signatures. *Journal of Systems and Software*, **2016**, 116, 95-100	3.3	18
40	Efficient Computation of Roots in Finite Fields. *Designs, Codes, and Cryptography*, **2006**, 39, 275-280	1.2	18
39	On Compressible Pairings and Their Computation **2008**, 371-388		18
38	The Realm of the Pairings. *Lecture Notes in Computer Science*, **2014**, 3-25	0.9	16
37	The Lattice-Based Digital Signature Scheme qTESLA. *Lecture Notes in Computer Science*, **2020**, 441-460	0.9	15
36	Monoidic Codes in Cryptography. *Lecture Notes in Computer Science*, **2011**, 179-199	0.9	14
35	. *IEEE Transactions on Computers*, **2019**, 68, 688-701	2.5	14
34	DAGS: Key encapsulation using dyadic GS codes. *Journal of Mathematical Cryptology*, **2018**, 12, 221-239	0.6	13
33	Lyra: password-based key derivation with tunable memory and processing costs. *Journal of Cryptographic Engineering*, **2014**, 4, 75-89	1.9	11
32	CAKE: Code-Based Algorithm for Key Encapsulation. *Lecture Notes in Computer Science*, **2017**, 207-226	0.9	11
31	Comparison of Authenticated-Encryption schemes in Wireless Sensor Networks **2011**,		11
30	Key reduction of McElieceUs cryptosystem using list decoding **2011**,		11

29	Faster Isogeny-Based Compressed Key Agreement. *Lecture Notes in Computer Science*, **2018**, 248-268	0.9	10
28	Scaling efficient code-based cryptosystems for embedded platforms. *Journal of Cryptographic Engineering*, **2014**, 4, 123-134	1.9	10
27	Quasi-Dyadic CFS Signatures. *Lecture Notes in Computer Science*, **2011**, 336-349	0.9	10
26	Hardware accelerators for pairing based cryptosystems. *IEE Proceedings - Information Security*, **2005** , 152, 47		10
25	Lyra2: Efficient Password Hashing with High Security against Time-Memory Trade-Offs. *IEEE Transactions on Computers*, **2016**, 65, 3096-3108	2.5	9
24	SMSCrypto: A lightweight cryptographic framework for secure SMS transmission. *Journal of Systems and Software*, **2013**, 86, 698-706	3.3	8
23	Improved Square Attacks against Reduced-Round Hierocrypt. *Lecture Notes in Computer Science*, **2002**, 165-173	0.9	8
22	Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds **2010**,		7
21	A flexible processor for the characteristic 3 □ pairing. *International Journal of High Performance Systems Architecture*, **2007**, 1, 79	0.9	7
20	Pitfalls in public key watermarking		7
19	Optimized and Scalable Co-Processor for McEliece with Binary Goppa Codes. *Transactions on Embedded Computing Systems*, **2015**, 14, 1-32	1.8	6
18	Toward a secure public-key blockwise fragile authentication watermarking		6
17	A Panorama of Post-quantum Cryptography **2014**, 387-439		5
16	Revisiting the Security of the ALRED Design and Two of Its Variants: Marvin and LetterSoup. *IEEE Transactions on Information Theory*, **2012**, 58, 6223-6238	2.8	3
15	Implementation of Multivariate Quadratic Quasigroup for Wireless Sensor Network. *Lecture Notes in Computer Science*, **2010**, 64-78	0.9	3
14	DAGS: Reloaded Revisiting Dyadic Key Encapsulation. *Lecture Notes in Computer Science*, **2019**, 69-85	0.9	2
13	Parallelism Level Analysis of Binary Field Multiplication on FPGAs **2015**,		2
12	Designing Efficient Dyadic Operations for Cryptographic Applications. *Journal of Mathematical Cryptology*, **2020**, 14, 95-109	0.6	2

List of Publications

11	Revisiting the Security of the Alred Design. *Lecture Notes in Computer Science*, **2011**, 69-83	0.9	2
10	Schnorr-Based Implicit Certification: Improving the Security and Efficiency of Vehicular Communications. *IEEE Transactions on Computers*, **2021**, 70, 393-399	2.5	2
9	Isogeny-Based Key Compression Without Pairings. *Lecture Notes in Computer Science*, **2021**, 131-154	0.9	2
8	Quantum-assisted QD-CFS signatures. *Journal of Computer and System Sciences*, **2015**, 81, 458-467	1	1
7	A class of safe and efficient binary Edwards curves. *Journal of Cryptographic Engineering*, **2018**, 8, 271-283	1.9	1
6	Decoding Square-Free Goppa Codes Over BBF_{p}. *IEEE Transactions on Information Theory*, **2013**, 59, 6851-6858	2.8	1
5	Cryptographic architecture for co-process on consumer electronics devices **2016**,		1
4	Security issues in Sarkar□s e-cash protocol. *Information Processing Letters*, **2015**, 115, 801-803	0.8	
3	A New Matrix Algebra for LWE Encryption. *IEEE Latin America Transactions*, **2015**, 13, 3038-3043	0.7	
2	Signcryption Schemes Based on the Diffie□Hellman Problem. *Information Security and Cryptography*, **2010**, 57-69	3.6	
1	Signcryption Schemes Based on Bilinear Maps. *Information Security and Cryptography*, **2010**, 71-97	3.6	