Paulo S L M Barreto

List of Publications by Year
in descending order

66 papers	3,578 citations	318942 23 h-index	198040 52 g-index
68 all docs	68 docs citations	68 times ranked	1653 citing authors

#	Article	IF	Citations
1	Schnorr-Based Implicit Certification: Improving the Security and Efficiency of Vehicular Communications. IEEE Transactions on Computers, 2021, 70, 393-399.	2.4	3
2	Isogeny-Based Key Compression Without Pairings. Lecture Notes in Computer Science, 2021, , 131-154.	1.0	4
3	The Lattice-Based Digital Signature Scheme qTESLA. Lecture Notes in Computer Science, 2020, , 441-460.	1.0	26
4	Designing Efficient Dyadic Operations for Cryptographic Applications. Journal of Mathematical Cryptology, 2020, 14, 95-109.	0.4	3
5	DAGS: Reloaded Revisiting Dyadic Key Encapsulation. Lecture Notes in Computer Science, 2019, , 69-85.	1.0	3
6	Faster Key Compression for Isogeny-Based Cryptosystems. IEEE Transactions on Computers, 2019, 68, 688-701.	2.4	19
7	Faster Isogeny-Based Compressed Key Agreement. Lecture Notes in Computer Science, 2018, , 248-268.	1.0	11
8	A class of safe and efficient binary Edwards curves. Journal of Cryptographic Engineering, 2018, 8, 271-283.	1.5	1
9	DAGS: Key encapsulation using dyadic GS codes. Journal of Mathematical Cryptology, 2018, 12, 221-239.	0.4	18
10	CAKE: Code-Based Algorithm for Key Encapsulation. Lecture Notes in Computer Science, 2017, , 207-226.	1.0	13
11	Cryptographic architecture for co-process on consumer electronics devices. , 2016, , .		1
12	Lyra2: Efficient Password Hashing with High Security against Time-Memory Trade-Offs. IEEE Transactions on Computers, 2016, 65, 3096-3108.	2.4	11
13	Shorter hash-based signatures. Journal of Systems and Software, 2016, 116, 95-100.	3.3	24
14	Parallelism Level Analysis of Binary Field Multiplication on FPGAs. , 2015, , .		2
15	A New Matrix Algebra for LWE Encryption. IEEE Latin America Transactions, 2015, 13, 3038-3043.	1.2	0
16	Security issues in Sarkar's e-cash protocol. Information Processing Letters, 2015, 115, 801-803.	0.4	0
17	Optimized and Scalable Co-Processor for McEliece with Binary Goppa Codes. Transactions on Embedded Computing Systems, 2015, 14, 1-32.	2.1	11
18	Quantum-assisted QD-CFS signatures. Journal of Computer and System Sciences, 2015, 81, 458-467.	0.9	3

#	Article	IF	Citations
19	Subgroup Security in Pairing-Based Cryptography. Lecture Notes in Computer Science, 2015, , 245-265.	1.0	27
20	Scalable hardware implementation for Quasi-Dyadic Goppa encoder. , 2014, , .		0
21	A Panorama of Post-quantum Cryptography. , 2014, , 387-439.		5
22	Lyra: password-based key derivation with tunable memory and processing costs. Journal of Cryptographic Engineering, 2014, 4, 75-89.	1.5	12
23	Scaling efficient code-based cryptosystems for embedded platforms. Journal of Cryptographic Engineering, 2014, 4, 123-134.	1.5	15
24	The Realm of the Pairings. Lecture Notes in Computer Science, 2014, , 3-25.	1.0	24
25	SMSCrypto: A lightweight cryptographic framework for secure SMS transmission. Journal of Systems and Software, 2013, 86, 698-706.	3.3	10
26	Decoding Square-Free Goppa Codes Over BBF_{p}. IEEE Transactions on Information Theory, 2013, 59, 6851-6858.	1.5	1
27	Survey and comparison of message authentication solutions on wireless sensor networks. Ad Hoc Networks, 2013, 11, 1221-1236.	3.4	30
28	MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. , 2013, , .		250
29	Dynamic method to evaluate code optimization effectiveness. , 2012, , .		1
30	Revisiting the Security of the ALRED Design and Two of Its Variants: Marvin and LetterSoup. IEEE Transactions on Information Theory, 2012, 58, 6223-6238.	1.5	3
31	Quasi-Dyadic CFS Signatures. Lecture Notes in Computer Science, 2011, , 336-349.	1.0	13
32	Comparison of Authenticated-Encryption schemes in Wireless Sensor Networks. , 2011, , .		17
33	Key reduction of McEliece's cryptosystem using list decoding. , 2011, , .		14
34	One-time signature scheme from syndrome decoding over generic error-correcting codes. Journal of Systems and Software, 2011, 84, 198-204.	3.3	20
35	A family of implementation-friendly BN elliptic curves. Journal of Systems and Software, 2011, 84, 1319-1326.	3.3	68
36	Revisiting the Security of the Alred Design. Lecture Notes in Computer Science, 2011, , 69-83.	1.0	2

#	Article	IF	Citations
37	Monoidic Codes in Cryptography. Lecture Notes in Computer Science, 2011, , 179-199.	1.0	21
38	Whirlwind: a new cryptographic hash function. Designs, Codes, and Cryptography, 2010, 56, 141-162.	1.0	25
39	A survey on key management mechanisms for distributed Wireless Sensor Networks. Computer Networks, 2010, 54, 2591-2612.	3.2	170
40	Implementation of Multivariate Quadratic Quasigroup for Wireless Sensor Network. Lecture Notes in Computer Science, 2010, , 64-78.	1.0	4
41	Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds. , 2010, , .		13
42	Signcryption Schemes Based on the Diffieâ€“Hellman Problem. Information Security and Cryptography, 2010, , 57-69.	0.2	1
43	Signcryption Schemes Based on Bilinear Maps. Information Security and Cryptography, 2010, , 71-97.	0.2	1
44	Providing Integrity and Authenticity in DICOM Images: A Novel Approach. IEEE Transactions on Information Technology in Biomedicine, 2009, 13, 582-589.	3.6	66
45	Compact McEliece Keys from Goppa Codes. Lecture Notes in Computer Science, 2009, , 376-392.	1.0	106
46	The M<scp>ARVIN</scp> message authentication code and the L<scp>ETTER</scp>S<scp>OUP</scp> authenticated encryption scheme. Security and Communication Networks, 2009, 2, 165-180.	1.0	22
47	Rotation symmetry in algebraically generated cryptographic substitution tables. Information Processing Letters, 2008, 106, 246-250.	0.4	26
48	On Compressible Pairings and Their Computation. , 2008, , 371-388.		23
49	A flexible processor for the characteristic 3 Î·<SUB align=right>T pairing. International Journal of High Performance Systems Architecture, 2007, 1, 79.	0.2	9
50	Efficient pairing computation on supersingular Abelian varieties. Designs, Codes, and Cryptography, 2007, 42, 239-271.	1.0	286
51	Pairing-Friendly Elliptic Curves of Prime Order. Lecture Notes in Computer Science, 2006, , 319-331.	1.0	475
52	Generating More MNT Elliptic Curves. Designs, Codes, and Cryptography, 2006, 38, 209-217.	1.0	46
53	Efficient Computation of Roots in Finite Fields. Designs, Codes, and Cryptography, 2006, 39, 275-280.	1.0	24
54	Hardware accelerators for pairing based cryptosystems. IEE Proceedings - Information Security, 2005, 152, 47.	1.9	12

#	Article	IF	Citations
55	A New Two-Party Identity-Based Authenticated Key Agreement. Lecture Notes in Computer Science, 2005, , 262-274.	1.0	135
56	Efficient Hardware for the Tate Pairing Calculation in Characteristic Three. Lecture Notes in Computer Science, 2005, , 412-426.	1.0	65
57	Compressed Pairings. Lecture Notes in Computer Science, 2004, , 140-156.	1.0	55
58	Efficient Implementation of Pairing-Based Cryptosystems. Journal of Cryptology, 2004, 17, 321-334.	2.1	114
59	On the Selection of Pairing-Friendly Groups. Lecture Notes in Computer Science, 2004, , 17-25.	1.0	85
60	Constructing Elliptic Curves with Prescribed Embedding Degrees. Lecture Notes in Computer Science, 2003, , 257-267.	1.0	125
61	Efficient Algorithms for Pairing-Based Cryptosystems. Lecture Notes in Computer Science, 2002, , 354-369.	1.0	618
62	Toward secure public-key blockwise fragile authentication watermarking. IET Computer Vision, 2002, 149, 57.	1.3	91
63	Improved Square Attacks against Reduced-Round Hierocrypt. Lecture Notes in Computer Science, 2002, , 165-173.	1.0	10
64	Fast binary image resolution increasing by k-nearest neighbor learning. , 2000, , .		2
65	Pitfalls in public key watermarking. , 0, , .		10
66	Toward a secure public-key blockwise fragile authentication watermarking. , 0, , .		17