Dan Boneh

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10652879/publications.pdf

Version: 2024-02-01

49 papers	18,126 citations	117625 34 h-index	302126 39 g-index
53 all docs	53 docs citations	53 times ranked	4524 citing authors

#	Article	IF	Citations
1	Identity-Based Encryption from the Weil Pairing. Lecture Notes in Computer Science, 2001, , 213-229.	1.3	3,953
2	Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing, 2003, 32, 586-615.	1.0	2,051
3	Short Signatures from the Weil Pairing. Lecture Notes in Computer Science, 2001, , 514-532.	1.3	1,595
4	Short Group Signatures. Lecture Notes in Computer Science, 2004, , 41-55.	1.3	1,196
5	Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. Lecture Notes in Computer Science, 2004, , 223-238.	1.3	1,118
6	Short Signatures from the Weil Pairing. Journal of Cryptology, 2004, 17, 297-319.	2.8	993
7	Short Signatures Without Random Oracles. Lecture Notes in Computer Science, 2004, , 56-73.	1.3	881
8	Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. Lecture Notes in Computer Science, 2005, , 258-275.	1.3	635
9	Efficient Lattice (H)IBE in the Standard Model. Lecture Notes in Computer Science, 2010, , 553-572.	1.3	605
10	Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. Journal of Cryptology, 2008, 21, 149-177.	2.8	462
11	On the Importance of Eliminating Errors in Cryptographic Computations. Journal of Cryptology, 2001, 14, 101-119.	2.8	405
12	Secure Identity Based Encryption Without Random Oracles. Lecture Notes in Computer Science, 2004, , 443-459.	1.3	381
13	Terra. , 2003, , .		378
14	Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits. Lecture Notes in Computer Science, 2014, , 533-556.	1.3	259
15	Constrained Pseudorandom Functions and Their Applications. Lecture Notes in Computer Science, 2013, , 280-300.	1.3	240
16	Chosenâ€Ciphertext Security from Identityâ€Based Encryption. SIAM Journal on Computing, 2007, 36, 1301-1328.	1.0	220
17	Signing a Linear Subspace: Signature Schemes for Network Coding. Lecture Notes in Computer Science, 2009, , 68-87.	1.3	218
18	Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys. Lecture Notes in Computer Science, 2006, , 573-592.	1.3	186

#	Article	IF	Citations
19	Homomorphic Signatures for Polynomial Functions. Lecture Notes in Computer Science, 2011, , 149-168.	1.3	176
20	Architectural support for copy and tamper resistant software. , 2000, , .		145
21	Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation. Lecture Notes in Computer Science, 2014, , 480-499.	1.3	144
22	Strongly Unforgeable Signatures Based on Computational Diffie-Hellman. Lecture Notes in Computer Science, 2006, , 229-240.	1.3	138
23	Efficient Selective Identity-Based Encryption WithoutÂRandom Oracles. Journal of Cryptology, 2011, 24, 659-693.	2.8	125
24	A fully collusion resistant broadcast, trace, and revoke system. , 2006, , .		124
25	Deriving genomic diagnoses without revealing patient genomes. Science, 2017, 357, 692-695.	12.6	110
26	Functional encryption. Communications of the ACM, 2012, 55, 56-64.	4.5	103
27	Space-Efficient Identity Based EncryptionWithout Pairings. , 2007, , .		95
28	Threshold Cryptosystems from Threshold Fully Homomorphic Encryption. Lecture Notes in Computer Science, 2018, , 565-596.	1.3	90
29	Function-Private Identity-Based Encryption: Hiding the Function in Functional Encryption. Lecture Notes in Computer Science, 2013, , 461-478.	1.3	84
30	Traitor tracing with constant size ciphertext. , 2008, , .		82
31	Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles. Lecture Notes in Computer Science, 2006, , 226-243.	1.3	80
32	Low Overhead Broadcast Encryption from Multilinear Maps. Lecture Notes in Computer Science, 2014, , 206-223.	1.3	67
33	Space-Efficient Identity Based EncryptionWithout Pairings. , 2007, , .		46
34	On the Impossibility of Basing Identity Based Encryption on Trapdoor Permutations. , 2008, , .		45
35	Overshadow. Operating Systems Review (ACM), 2008, 42, 2-13.	1.9	44
36	Privacy, Discovery, and Authentication for the Internet of Things. Lecture Notes in Computer Science, 2016, , 301-319.	1.3	44

#	Article	IF	Citations
37	Oblivious signature-based envelope. Distributed Computing, 2005, 17, 293-302.	0.8	42
38	Breaking generalized Diffieâ€“Hellman modulo a composite is no easier than factoring. Information Processing Letters, 1999, 70, 83-87.	0.6	39
39	Function-Private Subspace-Membership Encryption and Its Applications. Lecture Notes in Computer Science, 2013, , 255-275.	1.3	37
40	Symmetric Cryptography in Javascript. , 2009, , .		34
41	Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation. Algorithmica, 2017, 79, 1233-1285.	1.3	30
42	Computing on Authenticated Data. Journal of Cryptology, 2015, 28, 351-395.	2.8	22
43	T/Key. , 2017, , .		20
44	Multiparty Non-Interactive Key Exchange and More From Isogenies on Elliptic Curves. Journal of Mathematical Cryptology, 2020, 14, 5-14.	0.7	9
45	A Brief Look at Pairings Based Cryptography. , 2007, , .		6
46	Constrained Keys for Invertible Pseudorandom Functions. Lecture Notes in Computer Science, 2017, , 237-263.	1.3	6
47	Surnaming Schemes, Fast Verification, and Applications to SGX Technology. Lecture Notes in Computer Science, 2017, , 149-164.	1.3	5
48	BLS Short Digital Signatures. , 2011, , 158-159.		0
49	The Mobile Problem. , 0, , 169-196.		0