Masayuki Abe

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10867746/publications.pdf

Version: 2024-02-01

29	1,064	516710 16	526287 27
papers	citations	h-index	g-index

30	30	30	250
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Non-interactive Composition of Sigma-Protocols via Share-then-Hash. Lecture Notes in Computer Science, 2020, , 749-773.	1.3	7
2	On Black-Box Extensions of Non-interactive Zero-Knowledge Arguments, and Signatures Directly from Simulation Soundness. Lecture Notes in Computer Science, 2020, , 558-589.	1.3	4
3	On the Impossibility of Structure-Preserving Deterministic Primitives. Journal of Cryptology, 2019, 32, 239-264.	2.8	2
4	Efficient Fully Structure-Preserving Signatures and Shrinking Commitments. Journal of Cryptology, 2019, 32, 973-1025.	2.8	2
5	Shorter QA-NIZK and SPS with Tighter Security. Lecture Notes in Computer Science, 2019, , 669-699.	1.3	15
6	Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. Lecture Notes in Computer Science, 2018, , 3-22.	1.3	5
7	Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications. Lecture Notes in Computer Science, 2018, , 627-656.	1.3	20
8	Compact Structure-Preserving Signatures with Almost Tight Security. Lecture Notes in Computer Science, 2017, , 548-580.	1.3	29
9	Variations of Even-Goldreich-Micali Framework for Signature Schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 12-17.	0.3	0
10	Design in Type-I, Run in Type-III: Fast and Scalable Bilinear-Type Conversion Using Integer Programming. Lecture Notes in Computer Science, 2016, , 387-415.	1.3	12
11	Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions. Journal of Cryptology, 2016, 29, 833-878.	2.8	27
12	Structure-Preserving Signatures and Commitments to Group Elements. Journal of Cryptology, 2016, 29, 363-421.	2.8	39
13	Fully Structure-Preserving Signatures and Shrinking Commitments. Lecture Notes in Computer Science, 2015, , 35-65.	1.3	15
14	Tagged One-Time Signatures: Tight Security and Optimal Tag Size. Lecture Notes in Computer Science, 2013, , 312-331.	1.3	65
15	Double-trapdoor anonymous tags for traceable signatures. International Journal of Information Security, 2013, 12, 19-31.	3.4	15
16	Universally composable adaptive oblivious transfer (with access control) from standard assumptions. , 2013, , .		12
17	A framework for universally composable non-committing blind signatures. International Journal of Applied Cryptography, 2012, 2, 229.	0.4	8
18	Group to Group Commitments Do Not Shrink. Lecture Notes in Computer Science, 2012, , 301-317.	1.3	25

#	Article	IF	Citations
19	Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions. Lecture Notes in Computer Science, 2012, , 4-24.	1.3	68
20	Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. Lecture Notes in Computer Science, 2011, , 649-666.	1.3	99
21	Separating Short Structure-Preserving Signatures from Non-interactive Assumptions. Lecture Notes in Computer Science, 2011, , 628-646.	1.3	51
22	Efficient hybrid encryption from ID-based encryption. Designs, Codes, and Cryptography, 2010, 54, 205-240.	1.6	19
23	Structure-Preserving Signatures and Commitments to Group Elements. Lecture Notes in Computer Science, 2010, , 209-236.	1.3	223
24	Tag-KEM/DEM: A New Framework for Hybrid Encryption. Journal of Cryptology, 2008, 21, 97-130.	2.8	70
25	Chosen Ciphertext Security with Optimal Ciphertext Overhead. Lecture Notes in Computer Science, 2008, , 355-371.	1.3	19
26	Perfect NIZK with Adaptive Soundness. , 2007, , 118-136.		53
27	Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM. Lecture Notes in Computer Science, 2005, , 128-146.	1.3	94
28	Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography. Lecture Notes in Computer Science, 2004, , 317-334.	1.3	42
29	Robust Distributed Multiplication without Interaction. Lecture Notes in Computer Science, 1999, , 130-147.	1.3	21