Eike Kiltz

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7744783/publications.pdf

Version: 2024-02-01

27 papers	2,359 citations	304368 22 h-index	476904 29 g-index
30 all docs	30 docs citations	30 times ranked	703 citing authors

#	Article	IF	Citations
1	Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Journal of Cryptology, 2008, 21, 350-391.	2.1	247
2	A Modular Analysis of the Fujisaki-Okamoto Transformation. Lecture Notes in Computer Science, 2017, , 341-371.	1.0	224
3	An Algebraic Framework for Diffie-Hellman Assumptions. Lecture Notes in Computer Science, 2013, , 129-147.	1.0	203
4	Secure Hybrid Encryption from Weakened Key Encapsulation. , 2007, , 553-571.		190
5	Bonsai Trees, or How to Delegate a Lattice Basis. Journal of Cryptology, 2012, 25, 601-639.	2.1	146
6	The Algebraic Group Model and its Applications. Lecture Notes in Computer Science, 2018, , 33-62.	1.0	132
7	(Hierarchical) Identity-Based Encryption from Affine Message Authentication. Lecture Notes in Computer Science, 2014, , 408-425.	1.0	110
8	Programmable Hash Functions and Their Applications. Lecture Notes in Computer Science, 2008, , 21-38.	1.0	105
9	Quasi-Adaptive NIZK for Linear Subspaces Revisited. Lecture Notes in Computer Science, 2015, , 101-128.	1.0	79
10	Tightly CCA-Secure Encryption Without Pairings. Lecture Notes in Computer Science, 2016, , 1-27.	1.0	75
11	Message Authentication, Revisited. Lecture Notes in Computer Science, 2012, , 355-374.	1.0	65
12	A New Randomness Extraction Paradigm for Hybrid Encryption. Lecture Notes in Computer Science, 2009, , 590-609.	1.0	63
13	Efficient Authentication from Hard Learning Problems. Lecture Notes in Computer Science, 2011, , 7-26.	1.0	63
14	Bounded CCA2-Secure Encryption. Lecture Notes in Computer Science, 2007, , 502-518.	1.0	62
15	Tightly-Secure Authenticated Key Exchange. Lecture Notes in Computer Science, 2015, , 629-658.	1.0	59
16	The Twin Diffieâ€“Hellman Problem and Applications. Journal of Cryptology, 2009, 22, 470-504.	2.1	58
17	An Algebraic Framework for Diffieâ€“Hellman Assumptions. Journal of Cryptology, 2017, 30, 242-288.	2.1	58
18	Lapin: An Efficient Authentication Protocol Based on Ring-LPN. Lecture Notes in Computer Science, 2012, , 346-365.	1.0	45

#	Article	IF	Citations
19	Short Signatures from Weaker Assumptions. Lecture Notes in Computer Science, 2011, , 647-666.	1.0	43
20	Practical Chosen Ciphertext Secure Encryption from Factoring. Journal of Cryptology, 2013, 26, 102-118.	2.1	26
21	Lattice-Based Blind Signatures, Revisited. Lecture Notes in Computer Science, 2020, , 500-529.	1.0	23
22	A Modular Treatment of Blind Signatures from Identification Schemes. Lecture Notes in Computer Science, 2019, , 345-375.	1.0	22
23	Tightly-Secure Authenticated KeyÂExchange, Revisited. Lecture Notes in Computer Science, 2021, , 117-146.	1.0	18
24	Authenticated Key Exchange and Signatures with Tight Security in the Standard Model. Lecture Notes in Computer Science, 2021, , 670-700.	1.0	14
25	On the Impossibility of Purely Algebraic Signatures. Lecture Notes in Computer Science, 2021, , 317-349.	1.0	9
26	Efficient Authentication from Hard Learning Problems. Journal of Cryptology, 2017, 30, 1238-1275.	2.1	7
27	Everybodyâ€™s a Target: Scalability in Public-Key Encryption. Lecture Notes in Computer Science, 2020, , 475-506.	1.0	5