Sven SchÃ¤ge

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6557937/publications.pdf

Version: 2024-02-01

22 papers	452 citations	933447 10 h-index	752698 20 g-index
22 all docs	22 docs citations	22 times ranked	171 citing authors

#	Article	IF	Citations
1	On the Security of TLS-DHE in the Standard Model. Lecture Notes in Computer Science, 2012, , 273-293.	1.3	136
2	On the Impossibility of Tight Cryptographic Reductions. Lecture Notes in Computer Science, 2016, , 273-304.	1.3	57
3	Tight Proofs for Signature Schemes without Random Oracles. Lecture Notes in Computer Science, 2011, , 189-206.	1.3	38
4	Generic Authenticated Key Exchange inÂthe Quantum Random Oracle Model. Lecture Notes in Computer Science, 2020, , 389-422.	1.3	32
5	On the Security of the Pre-shared Key Ciphersuites of TLS. Lecture Notes in Computer Science, 2014, , 669-684.	1.3	26
6	A CDH-Based Ring Signature Scheme with Short Signatures and Public Keys. Lecture Notes in Computer Science, 2010, , 129-142.	1.3	23
7	Towards an Anonymous Access Control and Accountability Scheme for Cloud Computing. , 2010, , .		19
8	Tightly-Secure Authenticated KeyÂExchange, Revisited. Lecture Notes in Computer Science, 2021, , 117-146.	1.3	18
9	Generic Compilers for Authenticated Key Exchange. Lecture Notes in Computer Science, 2010, , 232-249.	1.3	18
10	Authenticated Key Exchange and Signatures with Tight Security in the Standard Model. Lecture Notes in Computer Science, 2021, , 670-700.	1.3	14
11	On the Selective Opening Security of Practical Public-Key Encryption Schemes. Lecture Notes in Computer Science, 2015, , 27-51.	1.3	14
12	Authenticated Confidential Channel Establishment and the Security of TLS-DHE. Journal of Cryptology, 2017, 30, 1276-1324.	2.8	10
13	On the Impossibility of Purely Algebraic Signatures. Lecture Notes in Computer Science, 2021, , 317-349.	1.3	9
14	Privacy-Preserving Authenticated Key Exchange and the Case of IKEv2. Lecture Notes in Computer Science, 2020, , 567-596.	1.3	8
15	TOPAS. , 2015, , .		6
16	Selective opening security of practical publicâ€key encryption schemes. IET Information Security, 2016, 10, 304-318.	1.7	6
17	New Modular Compilers for Authenticated Key Exchange. Lecture Notes in Computer Science, 2014, , 1-18.	1.3	6
18	Twin Signature Schemes, Revisited. Lecture Notes in Computer Science, 2009, , 104-117.	1.3	3

#	Article	IF	Citations
19	Strong Security from Probabilistic Signature Schemes. Lecture Notes in Computer Science, 2012, , 84-101.	1.3	3
20	Tight Security for Signature Schemes Without Random Oracles. Journal of Cryptology, 2015, 28, 641-670.	2.8	2
21	A New RSA-Based Signature Scheme. Lecture Notes in Computer Science, 2010, , 1-15.	1.3	2
22	Efficient Hash Collision Search Strategies on Special-Purpose Hardware. Lecture Notes in Computer Science, 2008, , 39-51.	1.3	2