

Jiaxin Pan

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/5965336/publications.pdf>

Version: 2024-02-01

26
papers

469
citations

840776

11
h-index

677142

22
g-index

26
all docs

26
docs citations

26
times ranked

155
citing authors

#	ARTICLE	IF	CITATIONS
1	(Hierarchical) Identity-Based Encryption from Affine Message Authentication. Lecture Notes in Computer Science, 2014, , 408-425.	1.3	110
2	Optimal Security Proofs for Signatures from Identification Schemes. Lecture Notes in Computer Science, 2016, , 33-61.	1.3	59
3	Structure-Preserving Signatures from Standard Assumptions, Revisited. Lecture Notes in Computer Science, 2015, , 275-295.	1.3	50
4	Tightly-Secure Signatures from Chameleon Hash Functions. Lecture Notes in Computer Science, 2015, , 256-279.	1.3	39
5	Compact Structure-Preserving Signatures with Almost Tight Security. Lecture Notes in Computer Science, 2017, , 548-580.	1.3	29
6	More Efficient (Almost) Tightly Secure Structure-Preserving Signatures. Lecture Notes in Computer Science, 2018, , 230-258.	1.3	29
7	Identity-Based Encryption Tightly Secure Under Chosen-Ciphertext Attacks. Lecture Notes in Computer Science, 2018, , 190-220.	1.3	20
8	Hierarchical Identity-Based Encryption with Tight Multi-challenge Security. Lecture Notes in Computer Science, 2020, , 153-183.	1.3	16
9	Shorter QA-NIZK and SPS with Tighter Security. Lecture Notes in Computer Science, 2019, , 669-699.	1.3	15
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	Tightly Secure Hierarchical Identity-Based Encryption. Lecture Notes in Computer Science, 2019, , 436-465.	1.3	13
12	Tightly Secure Hierarchical Identity-Based Encryption. Journal of Cryptology, 2020, 33, 1787-1821.	2.8	9
13	Lattice-Based Signatures with Tight Adaptive Corruptions and More. Lecture Notes in Computer Science, 2022, , 347-378.	1.3	9
14	Tightly-Secure Signatures from Five-Move Identification Protocols. Lecture Notes in Computer Science, 2017, , 68-94.	1.3	6
15	Fine-Grained Secure Attribute-Based Encryption. Lecture Notes in Computer Science, 2021, , 179-207.	1.3	6
16	Signed Diffie-Hellman Key Exchange with Tight Security. Lecture Notes in Computer Science, 2021, , 201-226.	1.3	6
17	Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH. Lecture Notes in Computer Science, 2018, , 490-518.	1.3	6
18	Unbounded HIBE with Tight Security. Lecture Notes in Computer Science, 2020, , 129-159.	1.3	6

#	ARTICLE	IF	CITATIONS
19	TMQV: A Strongly eCK-Secure Diffie-Hellman Protocol without Gap Assumption. Lecture Notes in Computer Science, 2011, , 380-388.	1.3	6
20	Signatures with Tight Multi-user Security from Search Assumptions. Lecture Notes in Computer Science, 2020, , 485-504.	1.3	5
21	Unified security model of authenticated key exchange with specific adversarial capabilities. IET Information Security, 2016, 10, 8-17.	1.7	4
22	Tightly secure signature schemes from the LWE and subset sum assumptions. Theoretical Computer Science, 2019, 795, 326-344.	0.9	3
23	Short Identity-Based Signatures with Tight Security from Lattices. Lecture Notes in Computer Science, 2021, , 360-379.	1.3	3
24	Analysis and Improvement of an Authenticated Key Exchange Protocol. Lecture Notes in Computer Science, 2011, , 417-431.	1.3	3
25	Non-Interactive Zero-Knowledge Proofs with Fine-Grained Security. Lecture Notes in Computer Science, 2022, , 305-335.	1.3	3
26	Security Enhancement and Modular Treatment towards Authenticated Key Exchange. Lecture Notes in Computer Science, 2010, , 203-217.	1.3	0