

Sanjit Chatterjee

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/10812055/publications.pdf>

Version: 2024-02-01

14
papers

228
citations

1307594

7
h-index

1125743

13
g-index

14
all docs

14
docs citations

14
times ranked

159
citing authors

#	ARTICLE	IF	CITATIONS
1	On cryptographic protocols employing asymmetric pairings “ The role of \hat{e} revisited. Discrete Applied Mathematics, 2011, 159, 1311-1322.	0.9	96
2	Comparing two pairing-based aggregate signature schemes. Designs, Codes, and Cryptography, 2010, 55, 141-167.	1.6	32
3	On the Efficiency and Security of Pairing-Based Protocols in the Type A1 and Type A4 Settings. Lecture Notes in Computer Science, 2010, , 114-134.	1.3	27
4	Variants of Waters’s Dual System Primitives Using Asymmetric Pairings. Lecture Notes in Computer Science, 2012, , 298-315.	1.3	20
5	Type 2 Structure-Preserving Signature Schemes Revisited. Lecture Notes in Computer Science, 2015, , 286-310.	1.3	17
6	Practical hybrid (hierarchical) identity-based encryption schemes based on the decisional bilinear Diffie-Hellman assumption. International Journal of Applied Cryptography, 2013, 3, 47.	0.4	11
7	On Instantiating Pairing-Based Protocols with Elliptic Curves of Embedding Degree One. IEEE Transactions on Computers, 2017, 66, 1061-1070.	3.4	8
8	Fault Attacks on Pairing-Based Protocols: Revisited. IEEE Transactions on Computers, 2014, , 1-1.	3.4	5
9	Efficient backward private searchable encryption. Journal of Computer Security, 2020, 28, 229-267.	0.8	4
10	Secure and efficient wildcard search over encrypted data. International Journal of Information Security, 2021, 20, 199-244.	3.4	3
11	Towards Static Assumption Based Cryptosystem in Pairing Setting: Further Applications of \hat{e} and Dual-Form Signature (Extended Abstract). Lecture Notes in Computer Science, 2018, , 220-238.	1.3	2
12	From Rerandomizability to Sequential Aggregation: Efficient Signature Schemes Based on SXDH Assumption. Lecture Notes in Computer Science, 2020, , 183-203.	1.3	2
13	Converting pairing-based cryptosystems from composite to prime order setting “ A comparative analysis. Journal of Mathematical Cryptology, 2018, 12, 159-190.	0.7	1
14	Efficient Protocol for Authenticated Email Search. Lecture Notes in Computer Science, 2015, , 1-20.	1.3	0