Mihir Bellare

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6590088/publications.pdf

Version: 2024-02-01

14	5,019	840119 11	1125271 13
papers	citations	h-index	g-index

16	16	16	1547
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Random oracles are practical. , 1993, , .		2,900
2	Relations among notions of security for public-key encryption schemes. Lecture Notes in Computer Science, 1998, , 26-45.	1.0	514
3	Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. Lecture Notes in Computer Science, 2000, , 259-274.	1.0	287
4	Authenticated Encryption: Relations among Notions andÂAnalysis of the Generic Composition Paradigm. Journal of Cryptology, 2008, 21, 469-491.	2.1	271
5	Efficient Garbling from a Fixed-Key Blockcipher. , 2013, , .		202
6	Security Proofs for Identity-Based Identification andÂSignature Schemes. Journal of Cryptology, 2009, 22, 1-61.	2.1	147
7	From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security. Lecture Notes in Computer Science, 2002, , 418-433.	1.0	120
8	Multirecipient Encryption Schemes: How to Save on Bandwidth and Computation Without Sacrificing Security. IEEE Transactions on Information Theory, 2007, 53, 3927-3943.	1.5	44
9	From Identification to Signatures Via the Fiatâ€“Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security. IEEE Transactions on Information Theory, 2008, 54, 3631-3646.	1.5	26
10	From Identification to Signatures, Tightly: A Framework and Generic Transforms. Lecture Notes in Computer Science, 2016, , 435-464.	1.0	24
11	Translucent Cryptographyâ€”An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer. Journal of Cryptology, 1999, 12, 117-139.	2.1	12
12	Efficient Schemes forÂCommitting Authenticated Encryption. Lecture Notes in Computer Science, 2022, , 845-875.	1.0	10
13	The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants. Lecture Notes in Computer Science, 2018, , 154-170.	1.0	9
14	Defending Against Key Exfiltration. , 2017, , .		7