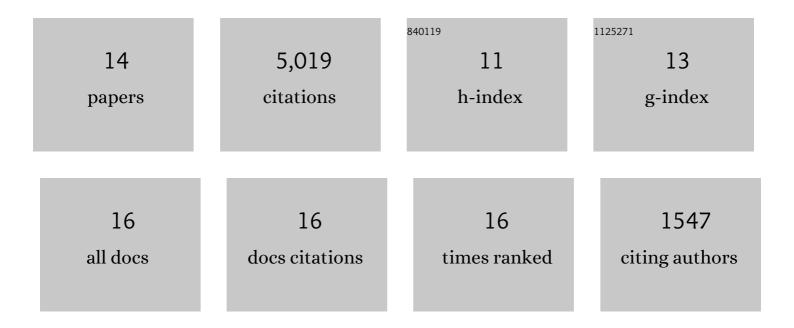
Mihir Bellare

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/6590088/publications.pdf Version: 2024-02-01



| # | Article | IF | CITATIONS |
|----|--|-----|-----------|
| 1 | Efficient Schemes forÂCommitting Authenticated Encryption. Lecture Notes in Computer Science, 2022, , 845-875. | 1.0 | 10 |
| 2 | The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants. Lecture Notes in Computer Science, 2018, , 154-170. | 1.0 | 9 |
| 3 | Defending Against Key Exfiltration. , 2017, , . | | 7 |
| 4 | From Identification to Signatures, Tightly: A Framework and Generic Transforms. Lecture Notes in Computer Science, 2016, , 435-464. | 1.0 | 24 |
| 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 | Authenticated Encryption: Relations among Notions andÂAnalysis of the Generic Composition Paradigm. Journal of Cryptology, 2008, 21, 469-491. | 2.1 | 271 |
| 8 | From Identification to Signatures Via the Fiat–Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security. IEEE Transactions on Information Theory, 2008, 54, 3631-3646. | 1.5 | 26 |
| 9 | 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 |
| 10 | 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 |
| 11 | Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. Lecture Notes in Computer Science, 2000, , 259-274. | 1.0 | 287 |
| 12 | Translucent Cryptography—An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer. Journal of Cryptology, 1999, 12, 117-139. | 2.1 | 12 |
| 13 | Relations among notions of security for public-key encryption schemes. Lecture Notes in Computer Science, 1998, , 26-45. | 1.0 | 514 |
| 14 | Random oracles are practical. , 1993, , . | | 2,900 |

2