# Michael Scott

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/11023483/publications.pdf

Version: 2024-02-01

| | | | |
|---|---|---|---|
| 20<br>papers | 2,430<br>citations | 516710<br>16<br>h-index | 839539<br>18<br>g-index |
| 21<br>all docs | 21<br>docs citations | 21<br>times ranked | 912<br>citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Efficient Algorithms for Pairing-Based Cryptosystems. Lecture Notes in Computer Science, 2002, , 354-369. | 1.3 | 618 |
| 2 | A Taxonomy of Pairing-Friendly Elliptic Curves. Journal of Cryptology, 2010, 23, 224-280. | 2.8 | 330 |
| 3 | Efficient pairing computation on supersingular Abelian varieties. Designs, Codes, and Cryptography, 2007, 42, 239-271. | 1.6 | 286 |
| 4 | NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. , 2008, , 305-320. | | 198 |
| 5 | TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 2011, 34, 485-493. | 5.1 | 190 |
| 6 | Efficient Implementation of Pairing-Based Cryptosystems. Journal of Cryptology, 2004, 17, 321-334. | 2.8 | 114 |
| 7 | Computing the Tate Pairing. Lecture Notes in Computer Science, 2005, , 293-304. | 1.3 | 102 |
| 8 | Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. Lecture Notes in Computer Science, 2008, , 126-135. | 1.3 | 91 |
| 9 | Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves. Journal of Cryptology, 2011, 24, 446-469. | 2.8 | 76 |
| 10 | TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. , 2008, , . | | 60 |
| 11 | On the Efficient Implementation of Pairing-Based Protocols. Lecture Notes in Computer Science, 2011, , 296-308. | 1.3 | 59 |
| 12 | Compressed Pairings. Lecture Notes in Computer Science, 2004, , 140-156. | 1.3 | 55 |
| 13 | Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions. Lecture Notes in Computer Science, 2010, , 209-223. | 1.3 | 48 |
| 14 | Generating More MNT Elliptic Curves. Designs, Codes, and Cryptography, 2006, 38, 209-217. | 1.6 | 46 |
| 15 | Exponentiation in Pairing-Friendly Groups Using Homomorphisms. Lecture Notes in Computer Science, 2008, , 211-224. | 1.3 | 38 |
| 16 | Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography. Lecture Notes in Computer Science, 2010, , 180-195. | 1.3 | 30 |
| 17 | Securing wireless sensor networks: an identity-based cryptography approach. International Journal of Sensor Networks, 2010, 8, 182. | 0.4 | 16 |
| 18 | FPGA acceleration of the tate pairing in characteristic 2. , 2006, , . | | 13 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | A New Family of Pairing-Friendly Elliptic Curves. Lecture Notes in Computer Science, 2018, , 43-57. | 1.3 | 7 |
| 20 | Designing a Code Generator for Pairing Based Cryptographic Functions. Lecture Notes in Computer Science, 2010, , 207-224. | 1.3 | 2 |