Michael Scott

List of Publications by Year
in descending order

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

#	ARTICLE	IF	CITATIONS
1	A New Family of Pairing-Friendly Elliptic Curves. Lecture Notes in Computer Science, 2018, , 43-57.	1.3	7
2	On the Efficient Implementation of Pairing-Based Protocols. Lecture Notes in Computer Science, 2011, , 296-308.	1.3	59
3	Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves. Journal of Cryptology, 2011, 24, 446-469.	2.8	76
4	TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 2011, 34, 485-493.	5.1	190
5	Securing wireless sensor networks: an identity-based cryptography approach. International Journal of Sensor Networks, 2010, 8, 182.	0.4	16
6	A Taxonomy of Pairing-Friendly Elliptic Curves. Journal of Cryptology, 2010, 23, 224-280.	2.8	330
7	Designing a Code Generator for Pairing Based Cryptographic Functions. Lecture Notes in Computer Science, 2010, , 207-224.	1.3	2
8	Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions. Lecture Notes in Computer Science, 2010, , 209-223.	1.3	48
9	Constructing Tower Extensions of Finite Fields for Implementation of Pairing-Based Cryptography. Lecture Notes in Computer Science, 2010, , 180-195.	1.3	30
10	NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. , 2008, , 305-320.		198
11	TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. , 2008, , .		60
12	Exponentiation in Pairing-Friendly Groups Using Homomorphisms. Lecture Notes in Computer Science, 2008, , 211-224.	1.3	38
13	Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. Lecture Notes in Computer Science, 2008, , 126-135.	1.3	91
14	Efficient pairing computation on supersingular Abelian varieties. Designs, Codes, and Cryptography, 2007, 42, 239-271.	1.6	286
15	FPGA acceleration of the tate pairing in characteristic 2. , 2006, , .		13
16	Generating More MNT Elliptic Curves. Designs, Codes, and Cryptography, 2006, 38, 209-217.	1.6	46
17	Computing the Tate Pairing. Lecture Notes in Computer Science, 2005, , 293-304.	1.3	102
18	Compressed Pairings. Lecture Notes in Computer Science, 2004, , 140-156.	1.3	55

#	Article	IF	Citations
19	Efficient Implementation of Pairing-Based Cryptosystems. Journal of Cryptology, 2004, 17, 321-334.	2.8	114
20	Efficient Algorithms for Pairing-Based Cryptosystems. Lecture Notes in Computer Science, 2002, , 354-369.	1.3	618