Aurore Guillevic

List of Publications by Year
in descending order

20 papers	298 citations	1163117 8 h-index	888059 17 g-index
20 all docs	20 docs citations	20 times ranked	144 citing authors

#	Article	IF	Citations
1	Comparing the Pairing Efficiency over Composite-Order and Prime-Order Elliptic Curves. Lecture Notes in Computer Science, 2013, , 357-372.	1.3	80
2	Improving NFS for the Discrete Logarithm Problem in Non-prime Finite Fields. Lecture Notes in Computer Science, 2015, , 129-155.	1.3	39
3	Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment. Lecture Notes in Computer Science, 2020, , 62-91.	1.3	28
4	A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-Bit Security Level. Lecture Notes in Computer Science, 2020, , 535-564.	1.3	25
5	Cocksâ€"Pinch curves of embedding degrees five to eight and optimal ate pairing computation. Designs, Codes, and Cryptography, 2020, 88, 1047-1081.	1.6	21
6	Four-Dimensional GLV via the Weil Restriction. Lecture Notes in Computer Science, 2013, , 79-96.	1.3	14
7	Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition. Lecture Notes in Computer Science, 2020, , 259-279.	1.3	12
8	Algorithms for Outsourcing Pairing Computation. Lecture Notes in Computer Science, 2015, , 193-211.	1.3	9
9	Families ofÂSNARK-Friendly 2-Chains ofÂElliptic Curves. Lecture Notes in Computer Science, 2022, , 367-396.	1.3	8
10	Faster individual discrete logarithms in finite fields of composite extension degree. Mathematics of Computation, 2018, 88, 1273-1301.	2.1	7
11	A New Family of Pairing-Friendly Elliptic Curves. Lecture Notes in Computer Science, 2018, , 43-57.	1.3	7
12	Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions. Lecture Notes in Computer Science, 2013, , 234-253.	1.3	7
13	Computing Individual Discrete Logarithms Faster in $${\mathrm{GF}}(p^n)$$ with the NFS-DL Algorithm. Lecture Notes in Computer Science, 2015, , 149-173.	1.3	7
14	The State of the Art in Integer Factoring and Breaking Public-Key Cryptography. IEEE Security and Privacy, 2022, 20, 80-86.	1.2	7
15	Efficient Multiplication in Finite Field Extensions of Degree 5. Lecture Notes in Computer Science, 2011, , 188-205.	1.3	6
16	Solving Discrete Logarithms on a 170-Bit MNT Curve by Pairing Reduction. Lecture Notes in Computer Science, 2017, , 559-578.	1.3	5
17	Computing Discrete Logarithms in $${\mathbb F}_{{p}^{6}}$$. Lecture Notes in Computer Science, 2018, , 85-105.	1.3	5
18	Isogenies for Point Counting on Genus Two Hyperelliptic Curves with Maximal Real Multiplication. Association for Women in Mathematics Series, 2017, , 63-94.	0.4	4

#	Article	IF	Citations
19	Automated fragment formula annotation for electron ionisation, high resolution mass spectrometry: application to atmospheric measurements of halocarbons. Journal of Cheminformatics, 2021, 13, 78.	6.1	4
20	Improved Broadcast Encryption Scheme with Constant-Size Ciphertext. Lecture Notes in Computer Science, 2013, , 196-202.	1.3	3