Paul Zimmermann

List of Publications by Year
in descending order

17	1,304	1162367 8	1125271 13
papers	citations	h-index	g-index

18	18	18	890
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	The State of the Art in Integer Factoring and Breaking Public-Key Cryptography. IEEE Security and Privacy, 2022, 20, 80-86.	1.5	7
2	Comparing the Difficulty of Factorization and Discrete Logarithm: A 240-Digit Experiment. Lecture Notes in Computer Science, 2020, , 62-91.	1.0	28
3	Imperfect forward secrecy. Communications of the ACM, 2018, 62, 106-114.	3.3	7
4	On Various Ways to Split a Floating-Point Number. , 2018, , .		7
5	Optimized Binary64 and Binary128 Arithmetic with GNU MPFR. , 2017, , .		3
6	Imperfect Forward Secrecy. , 2015, , .		238
7	Better polynomials for GNFS. Mathematics of Computation, 2015, 85, 861-873.	1.1	7
8	Discrete Logarithm in GF(2809) with FFS. Lecture Notes in Computer Science, 2014, , 221-238.	1.0	13
9	Finding Optimal Formulae for Bilinear Maps. Lecture Notes in Computer Science, 2012, , 168-186.	1.0	12
10	Short Division of Long Integers. , 2011, , .		0
11	Factorization of a 768-Bit RSA Modulus. Lecture Notes in Computer Science, 2010, , 333-350.	1.0	226
12	Reliable Computing with GNU MPFR. Lecture Notes in Computer Science, 2010, , 42-45.	1.0	6
13	Computing predecessor and successor in rounding toÂnearest. BIT Numerical Mathematics, 2009, 49, 419-431.	1.0	9
14	MPFR. ACM Transactions on Mathematical Software, 2007, 33, 13.	1.6	600
15	Proposal for a Standardization of Mathematical Function Implementation in Floating-Point Arithmetic. Numerical Algorithms, 2004, 37, 367-375.	1.1	13
16	The Middle Product Algorithm I. Applicable Algebra in Engineering, Communications and Computing, 2004, 14, 415-438.	0.3	43
17	Factorization of a 512-Bit RSA Modulus. Lecture Notes in Computer Science, 2000, , 1-18.	1.0	64