Tanja Lange

List of Publications by Year
in descending order

20 papers	2,421 citations	623734 14 h-index	794594 19 g-index
21 all docs	21 docs citations	21 times ranked	1378 citing authors

#	Article	IF	Citations
1	Post-quantum cryptography. Nature, 2017, 549, 188-194.	27.8	316
2	Flush, Gauss, and Reload â€“ A Cache Attack on the BLISS Lattice-Based Signature Scheme. Lecture Notes in Computer Science, 2016, , 323-345.	1.3	95
3	How to Manipulate Curve Standards: A White Paper for the Black Hat http://bada55.cr.yp.to. Lecture Notes in Computer Science, 2015, , 109-139.	1.3	30
4	Twisted Hessian Curves. Lecture Notes in Computer Science, 2015, , 269-294.	1.3	25
5	SPHINCS: Practical Stateless Hash-Based Signatures. Lecture Notes in Computer Science, 2015, , 368-397.	1.3	178
6	Hyper-and-elliptic-curve cryptography. LMS Journal of Computation and Mathematics, 2014, 17, 181-202.	0.9	14
7	Kummer Strikes Back: New DH Speed Records. Lecture Notes in Computer Science, 2014, , 317-337.	1.3	38
8	High-speed high-security signatures. Journal of Cryptographic Engineering, 2012, 2, 77-89.	1.8	322
9	Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Journal of Cryptology, 2008, 21, 350-391.	2.8	247
10	Twisted Edwards Curves. , 2008, , 389-405.		215
11	Attacking and Defending the McEliece Cryptosystem. Lecture Notes in Computer Science, 2008, , 31-46.	1.3	175
12	Distribution of some sequences of points on elliptic curves. Journal of Mathematical Cryptology, 2007, 1, 1-11.	0.7	28
13	Faster Addition and Doubling on Elliptic Curves. , 2007, , 29-50.		226
14	Koblitz curve cryptosystems. Finite Fields and Their Applications, 2005, 11, 200-229.	1.0	17
15	Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. Applicable Algebra in Engineering, Communications and Computing, 2005, 15, 295-328.	0.5	84
16	SCA Resistant Parallel Explicit Formula for Addition and Doubling of Divisors in the Jacobian of Hyperelliptic Curves of Genus 2. Lecture Notes in Computer Science, 2005, , 403-416.	1.3	4
17	Searchable Encryption Revisited:ÂConsistency Properties, Relation to Anonymous IBE, and Extensions. Lecture Notes in Computer Science, 2005, , 205-222.	1.3	357
18	On using expansions to the base of â˜2. International Journal of Computer Mathematics, 2004, 81, 403-406.	1.8	3

#	Article	IF	Citations
19	Montgomery Addition for Genus Two Curves. Lecture Notes in Computer Science, 2004, , 309-317.	1.3	4
20	Efficient Doubling on Genus Two Curves over Binary Fields. Lecture Notes in Computer Science, 2004, , 170-181.	1.3	30