Christophe Petit

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/8848062/publications.pdf

Version: 2024-02-01

		623574	434063
45	1,009	14	31
papers	citations	h-index	g-index
46	46	46	291
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. Lecture Notes in Computer Science, 2016, , 327-357.	1.0	174
2	On the Security of Supersingular Isogeny Cryptosystems. Lecture Notes in Computer Science, 2016, , 63-91.	1.0	115
3	Short Accountable Ring Signatures Based on DDH. Lecture Notes in Computer Science, 2015, , 243-265.	1.0	74
4	Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. Lecture Notes in Computer Science, 2017, , 3-33.	1.0	64
5	Faster Algorithms for Isogeny Problems Using Torsion Point Images. Lecture Notes in Computer Science, 2017, , 330-353.	1.0	57
6	On the quaternion -isogeny path problem. LMS Journal of Computation and Mathematics, 2014, 17, 418-432.	0.9	56
7	Verifiable Delay Functions from Supersingular Isogenies and Pairings. Lecture Notes in Computer Science, 2019, , 248-277.	1.0	52
8	SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. Lecture Notes in Computer Science, 2020, , 64-93.	1.0	52
9	Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions. Lecture Notes in Computer Science, 2018, , 329-368.	1.0	48
10	A block cipher based pseudo random number generator secure against side-channel key recovery. , 2008, , .		43
11	Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields. Lecture Notes in Computer Science, 2012, , 27-44.	1.0	35
12	On Polynomial Systems Arising from a Weil Descent. Lecture Notes in Computer Science, 2012, , 451-466.	1.0	29
13	Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. Journal of Cryptology, 2020, 33, 130-175.	2.1	21
14	Improved Torsion-Point Attacks on SIDH Variants. Lecture Notes in Computer Science, 2021, , 432-470.	1.0	18
15	Full Cryptanalysis of LPS and Morgenstern Hash Functions. Lecture Notes in Computer Science, 2008, , 263-277.	1.0	18
16	SÃ©ta: Supersingular Encryption fromÂTorsion Attacks. Lecture Notes in Computer Science, 2021, , 249-278.	1.0	17
17	Preimages for the Tillich-ZÃ©mor Hash Function. Lecture Notes in Computer Science, 2011, , 282-301.	1.0	12
18	Improvement of FaugÃ¨re et al.â€™s Method to Solve ECDLP. Lecture Notes in Computer Science, 2013, , 115-132.	1.0	12

#	Article	IF	Citations
19	Rubikâ€™s for Cryptographers. Notices of the American Mathematical Society, 2013, 60, 733.	0.1	11
20	Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields. Lecture Notes in Computer Science, 2016, , 3-18.	1.0	10
21	A Practical Cryptanalysis of WalnutDSA$$^{ext {TM}}$$. Lecture Notes in Computer Science, 2018, , 381-406.	1.0	9
22	First fall degree and Weil descent. Finite Fields and Their Applications, 2014, 30, 155-177.	0.6	8
23	One-Way Functions and Malleability Oracles: Hidden Shift Attacks onÂIsogeny-Based Protocols. Lecture Notes in Computer Science, 2021, , 242-271.	1.0	8
24	Hard and Easy Components of Collision Search in the ZÃ©mor-Tillich Hash Function: New Attacks and Reduced Variants with Equivalent Security. Lecture Notes in Computer Science, 2009, , 182-194.	1.0	7
25	Masking with Randomized Look Up Tables. Lecture Notes in Computer Science, 2012, , 283-299.	1.0	7
26	SimS: A Simplification of SiGamal. Lecture Notes in Computer Science, 2021, , 277-295.	1.0	5
27	On Adaptive Attacks Against Jao-Urbanikâ€™s Isogeny-Based Protocol. Lecture Notes in Computer Science, 2020, , 195-213.	1.0	5
28	Fault Attacks on Public Key Elements: Application to DLP-Based Schemes. , 2008, , 182-195.		5
29	Cayley Hash Functions. , 2011, , 183-184.		4
30	Another Look at Some Isogeny Hardness Assumptions. Lecture Notes in Computer Science, 2020, , 496-511.	1.0	4
31	SHealS andÂHealS: Isogeny-Based PKEs fromÂaÂKey Validation Method forÂSIDH. Lecture Notes in Computer Science, 2021, , 279-307.	1.0	4
32	Efficiency and pseudo-randomness of a variant of Z&#x00E9;mor-Tillich hash function. , 2008, , .		3
33	Towards factoring in $${SL(2,,mathbb{F}_{2^n})}$$. Designs, Codes, and Cryptography, 2014, 71, 409-431.	1.0	3
34	Quasi-subfield Polynomials and the Elliptic Curve Discrete Logarithm Problem. Journal of Mathematical Cryptology, 2020, 14, 25-38.	0.4	3
35	Finding roots in with the successive resultants algorithm. LMS Journal of Computation and Mathematics, 2014, 17, 203-217.	0.9	2
36	Cryptographic Hash Functions and Expander Graphs: The End of the Story?. Lecture Notes in Computer Science, 2016, , 304-311.	1.0	2

#	Article	IF	Citations
37	Full Cryptanalysis of Hash Functions Based on Cubic Ramanujan Graphs. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1891-1899.	0.2	2
38	Better path-finding algorithms in LPS Ramanujan graphs. Journal of Mathematical Cryptology, 2018, 12, 191-202.	0.4	2
39	Factoring Products of Braids via Garside Normal Form. Lecture Notes in Computer Science, 2019, , 646-678.	1.0	2
40	Semi-commutative Masking: A Framework for Isogeny-Based Protocols, with an Application to Fully Secure Two-Round Isogeny-Based OT. Lecture Notes in Computer Science, 2020, , 235-258.	1.0	2
41	A Generalised Successive Resultants Algorithm. Lecture Notes in Computer Science, 2016, , 105-124.	1.0	1
42	Supersingular isogeny graphs in cryptography. , 2019, , 143-166.		1
43	New results on quasi-subfield polynomials. Finite Fields and Their Applications, 2021, 75, 101881.	0.6	1
44	On a Particular Case of the Bisymmetric Equation for Quasigroups. Acta Mathematica Hungarica, 2014, 143, 330-336.	0.3	0
45	Torsion point attacks on â€˜SIDHâ€‘likeâ€™ cryptosystems. IET Information Security, 0, , .	1.1	0