Jintai Ding

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/7782913/publications.pdf

Version: 2024-02-01

25	989	777949 13	759306 22
papers	citations	h-index	g-index
27	27	27	278
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Efficient Key Recovery for All HFE Signature Variants. Lecture Notes in Computer Science, 2021, , 70-93.	1.0	12
2	Multivariate Public Key Cryptosystems. Advances in Information Security, 2020, , .	0.9	13
3	MQDSS. Advances in Information Security, 2020, , 153-168.	0.9	0
4	Solving Polynomial Systems. Advances in Information Security, 2020, , 185-248.	0.9	1
5	Multivariate Cryptography. Advances in Information Security, 2020, , 7-23.	0.9	0
6	The Matsumoto-Imai Cryptosystem. Advances in Information Security, 2020, , 25-60.	0.9	1
7	The SimpleMatrix Encryption Scheme. Advances in Information Security, 2020, , 169-183.	0.9	0
8	Oil and Vinegar. Advances in Information Security, 2020, , 89-151.	0.9	0
9	A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope. Lecture Notes in Computer Science, 2019, , 504-520.	1.0	15
10	Practical Randomized RLWE-Based Key Exchange Against Signal Leakage Attack. IEEE Transactions on Computers, 2018, 67, 1584-1593.	2.4	14
11	Fast Discretized Gaussian Sampling and Post-quantum TLS Ciphersuite. Lecture Notes in Computer Science, 2017, , 551-565.	1.0	2
12	Design Principles for HFEv- Based Multivariate Signature Schemes. Lecture Notes in Computer Science, 2015, , 311-334.	1.0	89
13	Simple Matrix â€“ A Multivariate Public Key Cryptosystem (MPKC) for Encryption. Finite Fields and Their Applications, 2015, 35, 352-368.	0.6	23
14	Authenticated Key Exchange from Ideal Lattices. Lecture Notes in Computer Science, 2015, , 719-751.	1.0	92
15	ZHFE, a New Multivariate Public Key Encryption Scheme. Lecture Notes in Computer Science, 2014, , 229-245.	1.0	53
16	Simple Matrix Scheme for Encryption. Lecture Notes in Computer Science, 2013, , 231-242.	1.0	59
17	GROWTH OF THE IDEAL GENERATED BY A QUADRATIC MULTIVARIATE FUNCTION OVER GF(3). Journal of Algebra and Its Applications, 2013, 12, 1250219.	0.3	3
18	Inverting HFE Systems Is Quasi-Polynomial for All Fields. Lecture Notes in Computer Science, 2011, , 724-742.	1.0	35

#	Article	IF	Citations
19	Towards Algebraic Cryptanalysis of HFE Challenge 2. Communications in Computer and Information Science, 2011, , 123-131.	0.4	6
20	SSE Implementation of Multivariate PKCs on Modern x86 CPUs. Lecture Notes in Computer Science, 2009, , 33-48.	1.0	66
21	New Differential-Algebraic Attacks and Reparametrization of Rainbow. Lecture Notes in Computer Science, 2008, , 242-257.	1.0	76
22	Inoculating Multivariate Schemes Against Differential Attacks. Lecture Notes in Computer Science, 2006, , 290-301.	1.0	21
23	Cryptanalysis of HFEv and Internal Perturbation of HFE. Lecture Notes in Computer Science, 2005, , 288-301.	1.0	39
24	Rainbow, a New Multivariable Polynomial Signature Scheme. Lecture Notes in Computer Science, 2005, , 164-175.	1.0	295
25	A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. Lecture Notes in Computer Science, 2004, , 305-318.	1.0	73