TancrÃ¨de Lepoint

List of Publications by Year
in descending order

Version: 2024-02-01

24 papers	1,643 citations	516215 16 h-index	676716 22 g-index
24 all docs	24 docs citations	24 times ranked	708 citing authors

#	Article	IF	Citations
1	Lattice Signatures and Bimodal Gaussians. Lecture Notes in Computer Science, 2013, , 40-56.	1.0	342
2	Practical Multilinear Maps over the Integers. Lecture Notes in Computer Science, 2013, , 476-493.	1.0	260
3	Batch Fully Homomorphic Encryption over the Integers. Lecture Notes in Computer Science, 2013, , 315-335.	1.0	189
4	Scale-Invariant Fully Homomorphic Encryption over the Integers. Lecture Notes in Computer Science, 2014, , 311-328.	1.0	99
5	A Comparison of the Homomorphic Encryption Schemes FV and YASHE. Lecture Notes in Computer Science, 2014, , 318-335.	1.0	92
6	Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations. Lecture Notes in Computer Science, 2015, , 247-266.	1.0	92
7	NFLlib: NTT-Based Fast Lattice Library. Lecture Notes in Computer Science, 2016, , 341-356.	1.0	78
8	New Multilinear Maps Over the Integers. Lecture Notes in Computer Science, 2015, , 267-286.	1.0	73
9	Two Attacks on a White-Box AES Implementation. Lecture Notes in Computer Science, 2014, , 265-285.	1.0	52
10	Improved Security Proofs in Lattice-Based Cryptography: Using the RÃ©nyi Divergence Rather Than the Statistical Distance. Lecture Notes in Computer Science, 2015, , 3-24.	1.0	51
11	Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. Journal of Cryptology, 2018, 31, 885-916.	2.1	51
12	Cryptanalysis of GGH15 Multilinear Maps. Lecture Notes in Computer Science, 2016, , 607-628.	1.0	50
13	Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression. Lecture Notes in Computer Science, 2016, , 313-333.	1.0	42
14	Improved Security Proofs in Lattice-Based Cryptography: Using the RÃ©nyi Divergence Rather than the Statistical Distance. Journal of Cryptology, 2018, 31, 610-640.	2.1	39
15	Zeroizing Attacks on Indistinguishability Obfuscation over CLT13. Lecture Notes in Computer Science, 2017, , 41-58.	1.0	33
16	White-Box Security Notions for Symmetric Encryption Schemes. Lecture Notes in Computer Science, 2014, , 247-264.	1.0	29
17	New Techniques for Obfuscating Conjunctions. Lecture Notes in Computer Science, 2019, , 636-666.	1.0	15
18	Partial Key Exposure on RSA with Private Exponents Larger Than N. Lecture Notes in Computer Science, 2012, , 369-380.	1.0	15

#	Article	IF	Citations
19	Cryptanalysis of a (Somewhat) Additively Homomorphic Encryption Scheme Used in PIR. Lecture Notes in Computer Science, 2015, , 184-193.	1.0	10
20	FHE over the Integers: Decomposed and Batched in the Post-Quantum Regime. Lecture Notes in Computer Science, 2017, , 271-301.	1.0	10
21	Optimization of Bootstrapping in Circuits. , 2017, , .		8
22	On the Minimal Number of Bootstrappings in Homomorphic Circuits. Lecture Notes in Computer Science, 2013, , 189-200.	1.0	8
23	Cryptanalysis of the Co-ACD Assumption. Lecture Notes in Computer Science, 2015, , 561-580.	1.0	3
24	Traitor tracing schemes for protected software implementations. , 2011, , .		2