Jonathan Katz

List of Publications by Year in descending order

45 papers	2,397 citations	318942 23 h-index	340414 39 g-index
46 all docs	46 docs citations	46 times ranked	1147 citing authors

#	Article	IF	Citations
1	Constant-Round Group Key Exchange from the Ring-LWE Assumption. Lecture Notes in Computer Science, 2019, , 189-205.	1.0	13
2	Synchronous Consensus with Optimal Asynchronous Fallback Guarantees. Lecture Notes in Computer Science, 2019, , 131-150.	1.0	23
3	Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. , 2018, , .		123
4	Verifiable Graph Processing. ACM Transactions on Privacy and Security, 2018, 21, 1-23.	2.2	2
5	An Expressive (Zero-Knowledge) Set Accumulator. , 2017, , .		15
6	Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited. Lecture Notes in Computer Science, 2017, , 473-495.	1.0	43
7	Automated Analysis and Synthesis of Block-Cipher Modes of Operation. , 2014, , .		21
8	Round-Optimal Password-Based Authenticated Key Exchange. Journal of Cryptology, 2013, 26, 714-743.	2.1	37
9	Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Journal of Cryptology, 2013, 26, 191-224.	2.1	106
10	Functional Encryption from (Small) Hardware Tokens. Lecture Notes in Computer Science, 2013, , 120-139.	1.0	5
11	Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IEEE Transactions on Information Theory, 2012, 58, 6207-6222.	1.5	63
12	Two-server password-only authenticated key exchange. Journal of Computer and System Sciences, 2012, 78, 651-669.	0.9	22
13	Partial Fairness in Secure Two-Party Computation. Journal of Cryptology, 2012, 25, 14-40.	2.1	23
14	Which Languages Have 4-Round Zero-Knowledge Proofs?. Journal of Cryptology, 2012, 25, 41-56.	2.1	8
15	Fair Computation with Rational Players. Lecture Notes in Computer Science, 2012, , 81-98.	1.0	53
16	On Achieving the â€œBest of Both Worldsâ€•in Secure Multiparty Computation. SIAM Journal on Computing, 2011, 40, 122-141.	0.8	23
17	Complete Fairness in Secure Two-Party Computation. Journal of the ACM, 2011, 58, 1-37.	1.8	46
18	Limits of Computational Differential Privacy in the Client/Server Setting. Lecture Notes in Computer Science, 2011, , 417-431.	1.0	14

#	Article	IF	Citations
19	Limits on the Power of Zero-Knowledge Proofs in Cryptographic Constructions. Lecture Notes in Computer Science, 2011, , 559-578.	1.0	23
20	Parallel and Concurrent Security of the HB and HB+ Protocols. Journal of Cryptology, 2010, 23, 402-421.	2.1	64
21	Bounds on the efficiency of black-box commitment schemes. Theoretical Computer Science, 2010, 411, 1251-1260.	0.5	1
22	Overcoming the Hole in the Bucket: Public-Key Cryptography Resilient to Continual Memory Leakage. , 2010, , .		134
23	Digital Signatures. , 2010, , .		68
24	Efficient and secure authenticated key exchange using weak passwords. Journal of the ACM, 2009, 57, 1-39.	1.8	64
25	Improving the round complexity of VSS in point-to-point networks. Information and Computation, 2009, 207, 889-899.	0.5	24
26	On expected constant-round protocols for Byzantine agreement. Journal of Computer and System Sciences, 2009, 75, 91-112.	0.9	51
27	Ring Signatures: Stronger Definitions, and Constructions without Random Oracles. Journal of Cryptology, 2009, 22, 114-138.	2.1	78
28	Reducing Complexity Assumptions forÂStatistically-Hiding Commitment. Journal of Cryptology, 2009, 22, 283-310.	2.1	4
29	On Black-Box Constructions of Predicate Encryption from Trapdoor Permutations. Lecture Notes in Computer Science, 2009, , 197-213.	1.0	12
30	Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices. Lecture Notes in Computer Science, 2009, , 636-652.	1.0	92
31	Handling Expected Polynomial-Time Strategies inÂSimulation-Based Security Proofs. Journal of Cryptology, 2008, 21, 303-349.	2.1	7
32	How to Encrypt with a Malicious Random Number Generator. Lecture Notes in Computer Science, 2008, , 303-315.	1.0	12
33	Round Complexity of Authenticated Broadcast with a Dishonest Majority. , 2007, , .		22
34	Scalable Protocols for Authenticated Group Key Exchange. Journal of Cryptology, 2007, 20, 85-113.	2.1	100
35	A Forward-Secure Public-Key Encryption Scheme. Journal of Cryptology, 2007, 20, 265-294.	2.1	101
36	Efficient Signature Schemes with Tight Reductions to the Diffie-Hellman Problems. Journal of Cryptology, 2007, 20, 493-514.	2.1	69

#	Article	IF	Citations
37	Round Complexity of Authenticated Broadcast with a Dishonest Majority. , 2007, , .		3
38	Characterization of Security Notions for Probabilistic Private-Key Encryption. Journal of Cryptology, 2006, 19, 67-95.	2.1	48
39	Parallel and Concurrent Security of the HB and HBâ€‰+â€‰ Protocols. Lecture Notes in Computer Science, 2006, , 73-87.	1.0	117
40	Universally Composable Password-Based Key Exchange. Lecture Notes in Computer Science, 2005, , 404-421.	1.0	169
41	Bounds on the Efficiency of Generic Cryptographic Constructions. SIAM Journal on Computing, 2005, 35, 217-246.	0.8	79
42	Secure Remote Authentication Using Biometric Data. Lecture Notes in Computer Science, 2005, , 147-163.	1.0	145
43	Reducing Complexity Assumptions for Statistically-Hiding Commitment. Lecture Notes in Computer Science, 2005, , 58-77.	1.0	23
44	Bounds on the Efficiency of â€œBlack-Boxâ€•Commitment Schemes. Lecture Notes in Computer Science, 2005, , 128-139.	1.0	6
45	One-Round Protocols for Two-Party Authenticated Key Exchange. Lecture Notes in Computer Science, 2004, , 220-232.	1.0	62