Gil Segev

List of Publications by Year
in descending order

45 papers	1,348 citations	471509 17 h-index	377865 34 g-index
45 all docs	45 docs citations	45 times ranked	541 citing authors

#	Article	IF	Citations
1	Public-Key Cryptosystems Resilient to Key Leakage. Lecture Notes in Computer Science, 2009, , 18-35.	1.3	261
2	Hedged Public-Key Encryption: How to Protect against Bad Randomness. Lecture Notes in Computer Science, 2009, , 232-249.	1.3	96
3	Message-Locked Encryption for Lock-Dependent Messages. Lecture Notes in Computer Science, 2013, , 374-391.	1.3	83
4	Public-Key Cryptosystems Resilient to Key Leakage. SIAM Journal on Computing, 2012, 41, 772-814.	1.0	71
5	Anonymous IBE, Leakage Resilience and Circular Security from New Assumptions. Lecture Notes in Computer Science, 2018, , 535-564.	1.3	67
6	Fully Leakage-Resilient Signatures. Lecture Notes in Computer Science, 2011, , 89-108.	1.3	61
7	Backyard Cuckoo Hashing: Constant Worst-Case Operations with a Succinct Representation. , 2010, , .		52
8	Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting. Lecture Notes in Computer Science, 2011, , 543-560.	1.3	52
9	Public-Key Cryptographic Primitives Provably as Secure as Subset Sum. Lecture Notes in Computer Science, 2010, , 382-400.	1.3	47
10	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		44
11	More Constructions of Lossy and Correlation-Secure Trapdoor Functions. Journal of Cryptology, 2013, 26, 39-74.	2.8	40
12	Incremental Deterministic Public-Key Encryption. Lecture Notes in Computer Science, 2012, , 628-644.	1.3	40
13	Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions. Lecture Notes in Computer Science, 2013, , 93-110.	1.3	38
14	A new approach to interdomain routing based on secure multi-party computation. , 2012, , .		37
15	Fully Leakage-Resilient Signatures. Journal of Cryptology, 2013, 26, 513-558.	2.8	33
16	Limits on the Power of Indistinguishability Obfuscation and Functional Encryption. , 2015, , .		32
17	Chosen-Ciphertext Security via Correlated Products. SIAM Journal on Computing, 2010, 39, 3058-3088.	1.0	29
18	Privacy-Preserving Interdomain Routing at Internet Scale. Proceedings on Privacy Enhancing Technologies, 2017, 2017, 147-167.	2.8	29

#	Article	IF	Citations
19	Finding Collisions in Interactive Protocols---Tight Lower Bounds on the Round and Communication Complexities of Statistically Hiding Commitments. SIAM Journal on Computing, 2015, 44, 193-242.	1.0	26
20	An Optimally Fair Coin Toss. Journal of Cryptology, 2016, 29, 491-513.	2.8	23
21	Function-Private Functional Encryption in the Private-Key Setting. Journal of Cryptology, 2018, 31, 202-225.	2.8	20
22	Sketching in Adversarial Environments. SIAM Journal on Computing, 2011, 40, 1845-1870.	1.0	18
23	Multi-input Functional Encryption in the Private-Key Setting: Stronger Security from Weaker Assumptions. Journal of Cryptology, 2018, 31, 434-520.	2.8	15
24	Limits on the Power of Indistinguishability Obfuscation and Functional Encryption. SIAM Journal on Computing, 2016, 45, 2117-2176.	1.0	14
25	Tight Tradeoffs in Searchable Symmetric Encryption. Journal of Cryptology, 2021, 34, 1.	2.8	13
26	On Constructing One-Way Permutations from Indistinguishability Obfuscation. Lecture Notes in Computer Science, 2016, , 512-541.	1.3	11
27	Incremental Deterministic Public-Key Encryption. Journal of Cryptology, 2018, 31, 134-161.	2.8	11
28	Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models. IEEE Transactions on Information Theory, 2008, 54, 2408-2425.	2.4	10
29	Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting. Journal of Cryptology, 2014, 27, 210-247.	2.8	10
30	Can PPAD Hardness be Based on Standard Cryptographic Assumptions?. Lecture Notes in Computer Science, 2017, , 747-776.	1.3	9
31	From Minicrypt to Obfustopia via Private-Key Functional Encryption. Journal of Cryptology, 2020, 33, 406-458.	2.8	9
32	Approximate k-Steiner Forests via the Lagrangian Relaxation Technique with Internal Preprocessing. Algorithmica, 2010, 56, 529-549.	1.3	6
33	Functional Encryption for Randomized Functionalities in the Private-Key Setting from Minimal Assumptions. Journal of Cryptology, 2018, 31, 60-100.	2.8	6
34	Securing Abeâ€™s Mix-Net Against Malicious Verifiers via Witness Indistinguishability. Lecture Notes in Computer Science, 2018, , 274-291.	1.3	5
35	Deterministic Public-Key Encryption for Adaptively-Chosen Plaintext Distributions. Journal of Cryptology, 2018, 31, 1012-1063.	2.8	4
36	Out-of-Band Authentication in Group Messaging: Computational, Statistical, Optimal. Lecture Notes in Computer Science, 2018, , 63-89.	1.3	4

#	Article	IF	Citations
37	The Security of Lazy Users in Out-of-Band Authentication. Lecture Notes in Computer Science, 2018, , 575-599.	1.3	4
38	Lossy Functions Do Not Amplify Well. Lecture Notes in Computer Science, 2012, , 458-475.	1.3	4
39	Accumulators in (and Beyond) Generic Groups: Non-trivial Batch Verification Requires Interaction. Lecture Notes in Computer Science, 2020, , 77-107.	1.3	4
40	On Constructing One-Way Permutations from Indistinguishability Obfuscation. Journal of Cryptology, 2018, 31, 698-736.	2.8	3
41	Can PPAD Hardness be Based on Standard Cryptographic Assumptions?. Journal of Cryptology, 2021, 34, 1.	2.8	3
42	Title is missing!. Theory of Computing, 2009, 5, 43-67.	0.5	2
43	Finding Collisions in Interactive Protocols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments. , 2007, , .		2
44	Injective Trapdoor Functions via Derandomization: How Strong is Rudichâ€™s Black-Box Barrier?. Journal of Cryptology, 2021, 34, 1.	2.8	0
45	The Security of Lazy Users in Out-of-Band Authentication. ACM Transactions on Privacy and Security, 2020, 23, 1-32.	3.0	0