Amit Sahai

List of Publications by Year
in descending order

39 papers	13,916 citations	304701 22 h-index	552766 26 g-index
39 all docs	39 docs citations	39 times ranked	3590 citing authors

#	Article	IF	Citations
1	How to Use Indistinguishability Obfuscation: Deniable Encryption, and More. SIAM Journal on Computing, 2021, 50, 857-908.	1.0	17
2	Self-Processing Private Sensor Data via Garbled Encryption. Proceedings on Privacy Enhancing Technologies, 2020, 2020, 434-460.	2.8	1
3	Leakage-Resilient Secret Sharing Against Colluding Parties. , 2019, , .		20
4	Non-Interactive Multiparty Computation Without Correlated Randomness. Lecture Notes in Computer Science, 2017, , 181-211.	1.3	24
5	Bounded-Communication Leakage Resilience via Parity-Resilient Circuits. , 2016, , .		16
6	Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. SIAM Journal on Computing, 2016, 45, 882-929.	1.0	128
7	Breaking the Three Round Barrier for Non-malleable Commitments. , 2016, , .		11
8	Functional Encryption for Turing Machines. Lecture Notes in Computer Science, 2016, , 125-153.	1.3	47
9	Private Interactive Communication Across an Adversarial Channel. IEEE Transactions on Information Theory, 2015, 61, 6860-6875.	2.4	5
10	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. Journal of Cryptology, 2015, 28, 820-843.	2.8	50
11	Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation. Lecture Notes in Computer Science, 2015, , 563-594.	1.3	136
12	Privacy preserving protocol for detecting genetic relatives using rare variants. Bioinformatics, 2014, 30, i204-i211.	4.1	10
13	Multi-input Functional Encryption. Lecture Notes in Computer Science, 2014, , 578-602.	1.3	202
14	Private interactive communication across an adversarial channel. , 2014, , .		8
15	Identifying genetic relatives without compromising privacy. Genome Research, 2014, 24, 664-672.	5.5	30
16	Efficient Coding for Interactive Communication. IEEE Transactions on Information Theory, 2014, 60, 1899-1913.	2.4	47
17	Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Journal of Cryptology, 2013, 26, 191-224.	2.8	106
18	Sequential Aggregate Signatures, Multisignatures, and Verifiably Encrypted Signatures Without Random Oracles. Journal of Cryptology, 2013, 26, 340-373.	2.8	26

#	Article	IF	Citations
19	New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM, 2012, 59, 1-35.	2.2	125
20	Functional encryption. Communications of the ACM, 2012, 55, 56-64.	4.5	103
21	On the (im)possibility of obfuscating programs. Journal of the ACM, 2012, 59, 1-48.	2.2	334
22	Efficient and Explicit Coding for Interactive Communication. , 2011, , .		53
23	Functional Encryption: Definitions and Challenges. Lecture Notes in Computer Science, 2011, , 253-273.	1.3	558
24	Efficient Non-interactive Secure Computation. Lecture Notes in Computer Science, 2011, , 406-425.	1.3	83
25	Worry-free encryption. , 2010, , .		108
26	Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 2010, , 62-91.	1.3	795
27	On the Computational Complexity of Coin Flipping. , 2010, , .		13
28	Revocation Systems with Very Small Private Keys. , 2010, , .		165
29	Zero-Knowledge Proofs from Secure Multiparty Computation. SIAM Journal on Computing, 2009, 39, 1121-1152.	1.0	80
30	Efficient Non-interactive Proof Systems for Bilinear Groups. , 2008, , 415-432.		598
31	Ciphertext-Policy Attribute-Based Encryption. , 2007, , .		3,071
32	Attribute-based encryption with non-monotonic access structures. , 2007, , .		613
33	Ring Signatures of Sub-linear Size Without Random Oracles. Lecture Notes in Computer Science, 2007, , 423-434.	1.3	66
34	Attribute-based encryption for fine-grained access control of encrypted data. , 2006, , .		3,146
35	Cryptography from Anonymity. , 2006, , .		77
36	Perfect Non-interactive Zero Knowledge for NP. Lecture Notes in Computer Science, 2006, , 339-358.	1.3	236

#	Article	IF	Citations
37	Sequential Aggregate Signatures and Multisignatures Without Random Oracles. Lecture Notes in Computer Science, 2006, , 465-485.	1.3	228
38	Fuzzy Identity-Based Encryption. Lecture Notes in Computer Science, 2005, , 457-473.	1.3	2,424
39	Robust Non-interactive Zero Knowledge. Lecture Notes in Computer Science, 2001, , 566-598.	1.3	156