Amit Sahai

List of Publications by Citations

39 papers	9,989 citations	27 h-index	39 g-index
39 ext. papers	11,488 ext. citations	1.9 avg, IF	6.43 L-index

#	Paper	IF	Citations
39	Attribute-based encryption for fine-grained access control of encrypted data **2006**,		2184
38	**2007**,		2071
37	Fuzzy Identity-Based Encryption. *Lecture Notes in Computer Science*, **2005**, 457-473	0.9	1596
36	Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. *Lecture Notes in Computer Science*, **2010**, 62-91	0.9	616
35	Efficient Non-interactive Proof Systems for Bilinear Groups **2008**, 415-432		511
34	Attribute-based encryption with non-monotonic access structures **2007**,		456
33	Functional Encryption: Definitions and Challenges. *Lecture Notes in Computer Science*, **2011**, 253-273	0.9	426
32	On the (im)possibility of obfuscating programs. *Journal of the ACM*, **2012**, 59, 1-48	2	256
31	Perfect Non-interactive Zero Knowledge for NP. *Lecture Notes in Computer Science*, **2006**, 339-358	0.9	191
30	Sequential Aggregate Signatures and Multisignatures Without Random Oracles. *Lecture Notes in Computer Science*, **2006**, 465-485	0.9	163
29	Multi-input Functional Encryption. *Lecture Notes in Computer Science*, **2014**, 578-602	0.9	157
28	Revocation Systems with Very Small Private Keys **2010**,		132
27	Robust Non-interactive Zero Knowledge. *Lecture Notes in Computer Science*, **2001**, 566-598	0.9	131
26	Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation. *Lecture Notes in Computer Science*, **2015**, 563-594	0.9	112
25	New Techniques for Noninteractive Zero-Knowledge. *Journal of the ACM*, **2012**, 59, 1-35	2	103
24	Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. *SIAM Journal on Computing*, **2016**, 45, 882-929	1.1	96
23	Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. *Journal of Cryptology*, **2013**, 26, 191-224	2.1	93

22	Worry-free encryption **2010**,		92
21	Functional encryption. *Communications of the ACM*, **2012**, 55, 56-64	2.5	76
20	Efficient Non-interactive Secure Computation. *Lecture Notes in Computer Science*, **2011**, 406-425	0.9	69
19	Zero-Knowledge Proofs from Secure Multiparty Computation. *SIAM Journal on Computing*, **2009**, 39, 1121-1152	1.1	61
18	Ring Signatures of Sub-linear Size Without Random Oracles. *Lecture Notes in Computer Science*, **2007**, 423-434	0.9	57
17	Cryptography from Anonymity **2006**,		52
16	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. *Journal of Cryptology*, **2015**, 28, 820-843	2.1	43
15	Efficient and Explicit Coding for Interactive Communication **2011**,		39
14	Functional Encryption for Turing Machines. *Lecture Notes in Computer Science*, **2016**, 125-153	0.9	39
13	Efficient Coding for Interactive Communication. *IEEE Transactions on Information Theory*, **2014**, 60, 1899-1913	2.3	32
12	Identifying genetic relatives without compromising privacy. *Genome Research*, **2014**, 24, 664-72	9.7	23
11	Sequential Aggregate Signatures, Multisignatures, and Verifiably Encrypted Signatures Without Random Oracles. *Journal of Cryptology*, **2013**, 26, 340-373	2.1	23
10	Non-Interactive Multiparty Computation Without Correlated Randomness. *Lecture Notes in Computer Science*, **2017**, 181-211	0.9	15
9	Leakage-Resilient Secret Sharing Against Colluding Parties **2019**,		15
8	Bounded-Communication Leakage Resilience via Parity-Resilient Circuits **2016**,		14
7	Breaking the Three Round Barrier for Non-malleable Commitments **2016**,		11
6	On the Computational Complexity of Coin Flipping **2010**,		10
5	Privacy preserving protocol for detecting genetic relatives using rare variants. *Bioinformatics*, **2014**, 30, i204-11	7.2	7

4	Private interactive communication across an adversarial channel **2014**,		6
3	. *IEEE Transactions on Information Theory*, **2015**, 61, 6860-6875	2.8	5
2	How to Use Indistinguishability Obfuscation: Deniable Encryption, and More. *SIAM Journal on Computing*, **2021**, 50, 857-908	1.1	5
1	Self-Processing Private Sensor Data via Garbled Encryption. *Proceedings on Privacy Enhancing Technologies*, **2020**, 2020, 434-460	3.2	1