

Amit Sahai

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/11627418/publications.pdf>

Version: 2024-02-01

39
papers

13,916
citations

304602

22
h-index

552653

26
g-index

39
all docs

39
docs citations

39
times ranked

3590
citing authors

#	ARTICLE	IF	CITATIONS
1	Attribute-based encryption for fine-grained access control of encrypted data. , 2006, , .		3,146
2	Ciphertext-Policy Attribute-Based Encryption. , 2007, , .		3,071
3	Fuzzy Identity-Based Encryption. Lecture Notes in Computer Science, 2005, , 457-473.	1.0	2,424
4	Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 2010, , 62-91.	1.0	795
5	Attribute-based encryption with non-monotonic access structures. , 2007, , .		613
6	Efficient Non-interactive Proof Systems for Bilinear Groups. , 2008, , 415-432.		598
7	Functional Encryption: Definitions and Challenges. Lecture Notes in Computer Science, 2011, , 253-273.	1.0	558
8	On the (im)possibility of obfuscating programs. Journal of the ACM, 2012, 59, 1-48.	1.8	334
9	Perfect Non-interactive Zero Knowledge for NP. Lecture Notes in Computer Science, 2006, , 339-358.	1.0	236
10	Sequential Aggregate Signatures and Multisignatures Without Random Oracles. Lecture Notes in Computer Science, 2006, , 465-485.	1.0	228
11	Multi-input Functional Encryption. Lecture Notes in Computer Science, 2014, , 578-602.	1.0	202
12	Revocation Systems with Very Small Private Keys. , 2010, , .		165
13	Robust Non-interactive Zero Knowledge. Lecture Notes in Computer Science, 2001, , 566-598.	1.0	156
14	Semantically Secure Order-Revealing Encryption: Multi-input Functional Encryption Without Obfuscation. Lecture Notes in Computer Science, 2015, , 563-594.	1.0	136
15	Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits. SIAM Journal on Computing, 2016, 45, 882-929.	0.8	128
16	New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM, 2012, 59, 1-35.	1.8	125
17	Worry-free encryption. , 2010, , .		108
18	Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. Journal of Cryptology, 2013, 26, 191-224.	2.1	106

#	ARTICLE	IF	CITATIONS
19	Functional encryption. Communications of the ACM, 2012, 55, 56-64.	3.3	103
20	Efficient Non-interactive Secure Computation. Lecture Notes in Computer Science, 2011, , 406-425.	1.0	83
21	Zero-Knowledge Proofs from Secure Multiparty Computation. SIAM Journal on Computing, 2009, 39, 1121-1152.	0.8	80
22	Cryptography from Anonymity. , 2006, , .		77
23	Ring Signatures of Sub-linear Size Without Random Oracles. Lecture Notes in Computer Science, 2007, , 423-434.	1.0	66
24	Efficient and Explicit Coding for Interactive Communication. , 2011, , .		53
25	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interactive Zero-Knowledge Proofs. Journal of Cryptology, 2015, 28, 820-843.	2.1	50
26	Efficient Coding for Interactive Communication. IEEE Transactions on Information Theory, 2014, 60, 1899-1913.	1.5	47
27	Functional Encryption for Turing Machines. Lecture Notes in Computer Science, 2016, , 125-153.	1.0	47
28	Identifying genetic relatives without compromising privacy. Genome Research, 2014, 24, 664-672.	2.4	30
29	Sequential Aggregate Signatures, Multisignatures, and Verifiably Encrypted Signatures Without Random Oracles. Journal of Cryptology, 2013, 26, 340-373.	2.1	26
30	Non-Interactive Multiparty Computation Without Correlated Randomness. Lecture Notes in Computer Science, 2017, , 181-211.	1.0	24
31	Leakage-Resilient Secret Sharing Against Colluding Parties. , 2019, , .		20
32	How to Use Indistinguishability Obfuscation: Deniable Encryption, and More. SIAM Journal on Computing, 2021, 50, 857-908.	0.8	17
33	Bounded-Communication Leakage Resilience via Parity-Resilient Circuits. , 2016, , .		16
34	On the Computational Complexity of Coin Flipping. , 2010, , .		13
35	Breaking the Three Round Barrier for Non-malleable Commitments. , 2016, , .		11
36	Privacy preserving protocol for detecting genetic relatives using rare variants. Bioinformatics, 2014, 30, i204-i211.	1.8	10

#	ARTICLE	IF	CITATIONS
37	Private interactive communication across an adversarial channel. , 2014, , .		8
38	Private Interactive Communication Across an Adversarial Channel. IEEE Transactions on Information Theory, 2015, 61, 6860-6875.	1.5	5
39	Self-Processing Private Sensor Data via Garbled Encryption. Proceedings on Privacy Enhancing Technologies, 2020, 2020, 434-460.	2.3	1