Jens Groth

List of Publications by Year in descending order

56 papers	4,898 citations	134610 34 h-index	198040 52 g-index
59 all docs	59 docs citations	59 times ranked	868 citing authors

#	Article	IF	Citations
1	Foundations of Fully Dynamic Group Signatures. Journal of Cryptology, 2020, 33, 1822-1870.	2.1	6
2	Linear-Time Arguments with Sublinear Verification from Tensor Codes. Lecture Notes in Computer Science, 2020, , 19-46.	1.0	19
3	Efficient Fully Structure-Preserving Signatures and Shrinking Commitments. Journal of Cryptology, 2019, 32, 973-1025.	2.1	2
4	Arya: Nearly Linear-Time Zero-Knowledge Proofs for Correct Program Execution. Lecture Notes in Computer Science, 2018, , 595-626.	1.0	17
5	Updatable and Universal Common Reference Strings with Applications toÂzk-SNARKs. Lecture Notes in Computer Science, 2018, , 698-728.	1.0	82
6	Sub-linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits. Lecture Notes in Computer Science, 2018, , 669-699.	1.0	48
7	Efficient Batch Zero-Knowledge Arguments for Low Degree Polynomials. Lecture Notes in Computer Science, 2018, , 561-588.	1.0	20
8	Snarky Signatures: Minimal Signatures of Knowledge from Simulation-Extractable SNARKs. Lecture Notes in Computer Science, 2017, , 581-612.	1.0	80
9	Towards a Classification of Non-interactive Computational Assumptions in Cyclic Groups. Lecture Notes in Computer Science, 2017, , 66-96.	1.0	10
10	Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability. Lecture Notes in Computer Science, 2017, , 336-365.	1.0	43
11	Efficient Zero-Knowledge Proof Systems. Lecture Notes in Computer Science, 2016, , 1-31.	1.0	2
12	Structure-Preserving Signatures and Commitments to Group Elements. Journal of Cryptology, 2016, 29, 363-421.	2.1	39
13	Foundations of Fully Dynamic Group Signatures. Lecture Notes in Computer Science, 2016, , 117-136.	1.0	65
14	On the Size of Pairing-Based Non-interactive Arguments. Lecture Notes in Computer Science, 2016, , 305-326.	1.0	418
15	Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. Lecture Notes in Computer Science, 2016, , 327-357.	1.0	174
16	Efficient Fully Structure-Preserving Signatures for Large Messages. Lecture Notes in Computer Science, 2015, , 239-259.	1.0	28
17	Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative Zero-Knowledge Proofs. Journal of Cryptology, 2015, 28, 820-843.	2.1	50
18	Short Accountable Ring Signatures Based on DDH. Lecture Notes in Computer Science, 2015, , 243-265.	1.0	74

#	Article	IF	Citations
19	Making Sigma-Protocols Non-interactive Without Random Oracles. Lecture Notes in Computer Science, 2015, , 650-670.	1.0	17
20	One-Out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin. Lecture Notes in Computer Science, 2015, , 253-280.	1.0	118
21	Cryptography in the Multi-string Model. Journal of Cryptology, 2014, 27, 506-543.	2.1	12
22	Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures. Lecture Notes in Computer Science, 2014, , 688-712.	1.0	38
23	Fine-Tuning Groth-Sahai Proofs. Lecture Notes in Computer Science, 2014, , 630-649.	1.0	44
24	Converting Cryptographic Schemes from Symmetric to Asymmetric Bilinear Groups. Lecture Notes in Computer Science, 2014, , 241-260.	1.0	24
25	Structure-Preserving Signatures from Type II Pairings. Lecture Notes in Computer Science, 2014, , 390-407.	1.0	24
26	Zero-Knowledge Argument for Polynomial Evaluation with Application to Blacklists. Lecture Notes in Computer Science, 2013, , 646-663.	1.0	29
27	Efficient Noninteractive Proof Systems for Bilinear Groups. SIAM Journal on Computing, 2012, 41, 1193-1232.	0.8	116
28	New Techniques for Noninteractive Zero-Knowledge. Journal of the ACM, 2012, 59, 1-35.	1.8	125
29	Efficient Zero-Knowledge Argument for Correctness of a Shuffle. Lecture Notes in Computer Science, 2012, , 263-280.	1.0	120
30	Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups. Lecture Notes in Computer Science, 2011, , 649-666.	1.0	99
31	Efficient Zero-Knowledge Arguments from Two-Tiered Homomorphic Commitments. Lecture Notes in Computer Science, 2011, , 431-448.	1.0	36
32	Separating Short Structure-Preserving Signatures from Non-interactive Assumptions. Lecture Notes in Computer Science, 2011, , 628-646.	1.0	51
33	A Verifiable Secret Shuffle of Homomorphic Encryptions. Journal of Cryptology, 2010, 23, 546-579.	2.1	59
34	Multi-query Computationally-Private Information Retrieval with Constant Communication Rate. Lecture Notes in Computer Science, 2010, , 107-123.	1.0	31
35	Structure-Preserving Signatures and Commitments to Group Elements. Lecture Notes in Computer Science, 2010, , 209-236.	1.0	223
36	Short Pairing-Based Non-interactive Zero-Knowledge Arguments. Lecture Notes in Computer Science, 2010, , 321-340.	1.0	251

#	Article	IF	Citations
37	Short Non-interactive Zero-Knowledge Proofs. Lecture Notes in Computer Science, 2010, , 341-358.	1.0	30
38	Pairing-Based Non-interactive Zero-Knowledge Proofs. Lecture Notes in Computer Science, 2010, , 206-206.	1.0	7
39	Linear Algebra with Sub-linear Zero-Knowledge Arguments. Lecture Notes in Computer Science, 2009, , 192-208.	1.0	62
40	Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle. , 2008, , 379-396.		58
41	Efficient Non-interactive Proof Systems for Bilinear Groups. , 2008, , 415-432.		598
42	Ring Signatures of Sub-linear Size Without Random Oracles. Lecture Notes in Computer Science, 2007, , 423-434.	1.0	66
43	Verifiable Shuffle of Large Size Ciphertexts. , 2007, , 377-392.		44
44	Cryptography in the Multi-string Model. , 2007, , 323-341.		45
45	Fully Anonymous Group Signatures Without Random Oracles. , 2007, , 164-180.		156
46	A Non-interactive Shuffle with Pairing Based Verifiability. , 2007, , 51-67.		41
47	Perfect Non-interactive Zero Knowledge for NP. Lecture Notes in Computer Science, 2006, , 339-358.	1.0	236
48	Non-interactive Zaps and New Techniques for NIZK. Lecture Notes in Computer Science, 2006, , 97-111.	1.0	129
49	Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures. Lecture Notes in Computer Science, 2006, , 444-459.	1.0	246
50	Non-interactive Zero-Knowledge Arguments for Voting. Lecture Notes in Computer Science, 2005, , 467-482.	1.0	83
51	Group Signatures: Better Efficiency and New Theoretical Aspects. Lecture Notes in Computer Science, 2005, , 120-133.	1.0	114
52	Cryptography in Subgroups of $mathbb{Z}_{n}^{*}$. Lecture Notes in Computer Science, 2005, , 50-65.	1.0	40
53	Rerandomizable and Replayable Adaptive Chosen Ciphertext Attack Secure Cryptosystems. Lecture Notes in Computer Science, 2004, , 152-170.	1.0	39
54	Evaluating Security of Voting Schemes in the Universal Composability Framework. Lecture Notes in Computer Science, 2004, , 46-60.	1.0	42

#	Article	IF	Citations
55	Non-interactive and reusable non-malleable commitment schemes. , 2003, , .		56
56	The Theory and Implementation of an Electronic Voting System. Advances in Information Security, 2003, , 77-99.	0.9	26