Jesper Buus Nielsen

List of Publications by Year
in descending order

81 papers	3,657 citations	218592 26 h-index	155592 55 g-index
84 all docs	84 docs citations	84 times ranked	1094 citing authors

#	Article	IF	Citations
1	Secure Multiparty Computation Goes Live. Lecture Notes in Computer Science, 2009, , 325-343.	1.0	321
2	Unconditionally Secure Constant-Rounds Multi-party Computation for Equality, Comparison, Bits and Exponentiation. Lecture Notes in Computer Science, 2006, , 285-304.	1.0	259
3	A New Approach to Practical Active-Secure Two-Party Computation. Lecture Notes in Computer Science, 2012, , 681-700.	1.0	245
4	Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. Lecture Notes in Computer Science, 2002, , 111-126.	1.0	210
5	Scalable and Unconditionally Secure Multiparty Computation. , 2007, , 572-590.		142
6	Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption. Lecture Notes in Computer Science, 2003, , 247-264.	1.0	134
7	Asynchronous Multiparty Computation: Theory and Implementation. Lecture Notes in Computer Science, 2009, , 160-179.	1.0	131
8	A generalization of Paillierâ€™s public-key system with applications to electronic voting. International Journal of Information Security, 2010, 9, 371-385.	2.3	122
9	Improved Non-committing Encryption Schemes Based on a General Complexity Assumption. Lecture Notes in Computer Science, 2000, , 432-450.	1.0	108
10	Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor. Lecture Notes in Computer Science, 2002, , 581-596.	1.0	100
11	Perfectly Secure Oblivious RAM without Random Oracles. Lecture Notes in Computer Science, 2011, , 144-163.	1.0	97
12	LEGO for Two-Party Secure Computation. Lecture Notes in Computer Science, 2009, , 368-386.	1.0	93
13	Continuous Non-malleable Codes. Lecture Notes in Computer Science, 2014, , 465-488.	1.0	84
14	Scalable Multiparty Computation with Nearly Optimal Work and Resilience. Lecture Notes in Computer Science, 2008, , 241-261.	1.0	74
15	Yes, There is an Oblivious RAM Lower Bound!. Lecture Notes in Computer Science, 2018, , 523-542.	1.0	67
16	OT-Combiners via Secure Computation. Lecture Notes in Computer Science, 2008, , 393-411.	1.0	57
17	MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions. Lecture Notes in Computer Science, 2013, , 537-556.	1.0	49
18	Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge. Lecture Notes in Computer Science, 2015, , 191-219.	1.0	45

#	Article	IF	Citations
19	Simplified Threshold RSA with Adaptive and Proactive Security. Lecture Notes in Computer Science, 2006, , 593-611.	1.0	41
20	Actively Secure Two-Party Evaluation of Any Quantum Operation. Lecture Notes in Computer Science, 2012, , 794-811.	1.0	39
21	The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited. Lecture Notes in Computer Science, 2017, , 167-187.	1.0	34
22	Robust Multiparty Computation with Linear Communication Complexity. Lecture Notes in Computer Science, 2006, , 463-482.	1.0	33
23	Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO. , 2017, , .		32
24	Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries. Lecture Notes in Computer Science, 2010, , 685-706.	1.0	31
25	Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures. Lecture Notes in Computer Science, 2019, , 510-539.	1.0	30
26	Maliciously Secure Oblivious Linear Function Evaluation with Constant Overhead. Lecture Notes in Computer Science, 2017, , 629-659.	1.0	28
27	Cryptographic Asynchronous Multi-party Computation with Optimal Resilience. Lecture Notes in Computer Science, 2005, , 322-340.	1.0	27
28	A Threshold Pseudorandom Function Construction and Its Applications. Lecture Notes in Computer Science, 2002, , 401-416.	1.0	26
29	Signature Schemes Secure against Hard-to-Invert Leakage. Lecture Notes in Computer Science, 2012, , 98-115.	1.0	26
30	Fast and Maliciously Secure Two-Party Computation Using the GPU. Lecture Notes in Computer Science, 2013, , 339-356.	1.0	23
31	Rate-1, Linear Time and Additively Homomorphic UC Commitments. Lecture Notes in Computer Science, 2016, , 179-207.	1.0	23
32	A Framework for Outsourcing of Secure Computation. , 2014, , .		22
33	YOSO: You Only Speak Once. Lecture Notes in Computer Science, 2021, , 64-93.	1.0	22
34	A Tamper and Leakage Resilient von Neumann Architecture. Lecture Notes in Computer Science, 2015, , 579-603.	1.0	22
35	TARDIS: A Foundation of Time-Lock Puzzles in UC. Lecture Notes in Computer Science, 2021, , 429-459.	1.0	21
36	Isolated Proofs of Knowledge and Isolated Zero Knowledge. , 2008, , 509-526.		21

#	Article	IF	Citations
37	On the Complexity of Additively Homomorphic UC Commitments. Lecture Notes in Computer Science, 2016, , 542-565.	1.0	21
38	Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security. Lecture Notes in Computer Science, 2002, , 449-464.	1.0	20
39	Asynchronous Multi-Party Computation with Quadratic Communication. Lecture Notes in Computer Science, 2008, , 473-485.	1.0	20
40	Lower and Upper Bounds for Deniable Public-Key Encryption. Lecture Notes in Computer Science, 2011, , 125-142.	1.0	20
41	Faster Maliciously Secure Two-Party Computation Using the GPU. Lecture Notes in Computer Science, 2014, , 358-379.	1.0	19
42	On the Communication Required for Unconditionally Secure Multiplication. Lecture Notes in Computer Science, 2016, , 459-488.	1.0	19
43	Secure Key Management in the Cloud. Lecture Notes in Computer Science, 2013, , 270-289.	1.0	18
44	From Passive to Covert Security at Low Cost. Lecture Notes in Computer Science, 2010, , 128-145.	1.0	18
45	Essentially Optimal Universally Composable Oblivious Transfer. Lecture Notes in Computer Science, 2009, , 318-335.	1.0	17
46	Compact VSS and Efficient Homomorphic UC Commitments. Lecture Notes in Computer Science, 2014, , 213-232.	1.0	17
47	Additively Homomorphic UC Commitments with Optimal Amortized Overhead. Lecture Notes in Computer Science, 2015, , 495-515.	1.0	17
48	Universally Composable Multiparty Computation with Partially Isolated Parties. Lecture Notes in Computer Science, 2009, , 315-331.	1.0	16
49	Continuously Non-malleable Codes with Split-State Refresh. Lecture Notes in Computer Science, 2018, , 121-139.	1.0	14
50	Fully Simulatable Quantum-Secure Coin-Flipping and Applications. Lecture Notes in Computer Science, 2011, , 21-40.	1.0	14
51	Predictable Arguments of Knowledge. Lecture Notes in Computer Science, 2017, , 121-150.	1.0	14
52	On the Number of Synchronous Rounds Sufficient for Authenticated Byzantine Agreement. Lecture Notes in Computer Science, 2009, , 449-463.	1.0	14
53	ReverseÂFirewallsÂforÂActivelyÂSecureÂMPCs. Lecture Notes in Computer Science, 2020, , 732-762.	1.0	13
54	Leakage-Resilient Signatures with Graceful Degradation. Lecture Notes in Computer Science, 2014, , 362-379.	1.0	13

#	Article	IF	Citations
55	On the theoretical gap between synchronous and asynchronous MPC protocols. , 2010, , .		12
56	DUPLO. , 2017, , .		12
57	Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation. Lecture Notes in Computer Science, 2015, , 456-468.	1.0	12
58	On the Necessary and Sufficient Assumptions for UC Computation. Lecture Notes in Computer Science, 2010, , 109-127.	1.0	11
59	Upper Bounds on the Communication Complexity of Optimally Resilient Cryptographic Multiparty Computation. Lecture Notes in Computer Science, 2005, , 79-99.	1.0	10
60	Afgjort: A Partially Synchronous Finality Layer for Blockchains. Lecture Notes in Computer Science, 2020, , 24-44.	1.0	10
61	Cross and Clean: Amortized Garbled Circuits with Constant Overhead. Lecture Notes in Computer Science, 2016, , 582-603.	1.0	9
62	Privacy-Enhancing Auctions Using Rational Cryptography. Lecture Notes in Computer Science, 2009, , 541-558.	1.0	9
63	On the Connection between Leakage Tolerance and Adaptive Security. Lecture Notes in Computer Science, 2013, , 497-515.	1.0	8
64	Signature Schemes Secure Against Hard-to-Invert Leakage. Journal of Cryptology, 2016, 29, 422-455.	2.1	8
65	Continuous Non-Malleable Codes in the 8-Split-State Model. Lecture Notes in Computer Science, 2019, , 531-561.	1.0	8
66	Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing. Lecture Notes in Computer Science, 2019, , 61-84.	1.0	8
67	Secure Protocols with Asymmetric Trust. , 2007, , 357-375.		7
68	Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model. Theoretical Computer Science, 2017, 660, 23-56.	0.5	6
69	Adaptive versus Static Security in the UC Model. Lecture Notes in Computer Science, 2014, , 10-28.	1.0	5
70	Non-malleable Codes with Split-State Refresh. Lecture Notes in Computer Science, 2017, , 279-309.	1.0	5
71	Unconditionally Secure Computation with Reduced Interaction. Lecture Notes in Computer Science, 2016, , 420-447.	1.0	5
72	On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation. Lecture Notes in Computer Science, 2015, , 87-104.	1.0	4

#	Article	IF	Citations
73	On the Computational Overhead of MPC with Dishonest Majority. Lecture Notes in Computer Science, 2017, , 369-395.	1.0	4
74	Improved Non-Committing Encryption Schemes based on a General Complexity Assumption. BRICS Report Series, 2000, 7, .	0.2	3
75	Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor. BRICS Report Series, 2001, 8, .	0.2	3
76	Continuously Non-malleable Codes in the Split-State Model. Journal of Cryptology, 2020, 33, 2034-2077.	2.1	2
77	High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer. Journal of Cryptology, 2021, 34, 1.	2.1	2
78	Weight-Based Nakamoto-Style Blockchains. Lecture Notes in Computer Science, 2021, , 299-319.	1.0	1
79	Reactive Garbling: Foundation, Instantiation, Application. Lecture Notes in Computer Science, 2016, , 1022-1052.	1.0	1
80	Fully Leakage-Resilient Codes. Lecture Notes in Computer Science, 2017, , 333-358.	1.0	1
81	Privacy-enhancing auctions using rational cryptography. , 2010, , .		0