

Jesper Buus Nielsen

List of Publications by Citations

Source: <https://exaly.com/author-pdf/5781290/jesper-buus-nielsen-publications-by-citations.pdf>

Version: 2024-04-28

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

82

papers

2,825

citations

24

h-index

51

g-index

84

ext. papers

3,122

ext. citations

0.9

avg, IF

5.52

L-index

#	Paper	IF	Citations
82	Secure Multiparty Computation Goes Live. <i>Lecture Notes in Computer Science</i> , 2009 , 325-343	0.9	245
81	A New Approach to Practical Active-Secure Two-Party Computation. <i>Lecture Notes in Computer Science</i> , 2012 , 681-700	0.9	206
80	Unconditionally Secure Constant-Rounds Multi-party Computation for Equality, Comparison, Bits and Exponentiation. <i>Lecture Notes in Computer Science</i> , 2006 , 285-304	0.9	194
79	Secure Multiparty Computation and Secret Sharing 2015 ,		193
78	Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. <i>Lecture Notes in Computer Science</i> , 2002 , 111-126	0.9	189
77	Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption. <i>Lecture Notes in Computer Science</i> , 2003 , 247-264	0.9	103
76	Scalable and Unconditionally Secure Multiparty Computation 2007 , 572-590		95
75	Improved Non-committing Encryption Schemes Based on a General Complexity Assumption. <i>Lecture Notes in Computer Science</i> , 2000 , 432-450	0.9	95
74	Asynchronous Multiparty Computation: Theory and Implementation. <i>Lecture Notes in Computer Science</i> , 2009 , 160-179	0.9	93
73	Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor. <i>Lecture Notes in Computer Science</i> , 2002 , 581-596	0.9	92
72	LEGO for Two-Party Secure Computation. <i>Lecture Notes in Computer Science</i> , 2009 , 368-386	0.9	79
71	A generalization of Paillier's public-key system with applications to electronic voting. <i>International Journal of Information Security</i> , 2010 , 9, 371-385	2.8	76
70	Continuous Non-malleable Codes. <i>Lecture Notes in Computer Science</i> , 2014 , 465-488	0.9	74
69	Perfectly Secure Oblivious RAM without Random Oracles. <i>Lecture Notes in Computer Science</i> , 2011 , 144-163		72
68	Scalable Multiparty Computation with Nearly Optimal Work and Resilience. <i>Lecture Notes in Computer Science</i> , 2008 , 241-261	0.9	59
67	OT-Combiners via Secure Computation. <i>Lecture Notes in Computer Science</i> , 2008 , 393-411	0.9	49
66	MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions. <i>Lecture Notes in Computer Science</i> , 2013 , 537-556	0.9	42

65	Yes, There is an Oblivious RAM Lower Bound!. <i>Lecture Notes in Computer Science</i> , 2018 , 523-542	0.9	39
64	Actively Secure Two-Party Evaluation of Any Quantum Operation. <i>Lecture Notes in Computer Science</i> , 2012 , 794-811	0.9	34
63	Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge. <i>Lecture Notes in Computer Science</i> , 2015 , 191-219	0.9	34
62	Simplified Threshold RSA with Adaptive and Proactive Security. <i>Lecture Notes in Computer Science</i> , 2006 , 593-611	0.9	31
61	The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited. <i>Lecture Notes in Computer Science</i> , 2017 , 167-187	0.9	28
60	Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries. <i>Lecture Notes in Computer Science</i> , 2010 , 685-706	0.9	28
59	Robust Multiparty Computation with Linear Communication Complexity. <i>Lecture Notes in Computer Science</i> , 2006 , 463-482	0.9	26
58	Superposition Attacks on Cryptographic Protocols. <i>Lecture Notes in Computer Science</i> , 2014 , 142-161	0.9	24
57	Cryptographic Asynchronous Multi-party Computation with Optimal Resilience. <i>Lecture Notes in Computer Science</i> , 2005 , 322-340	0.9	22
56	Signature Schemes Secure against Hard-to-Invert Leakage. <i>Lecture Notes in Computer Science</i> , 2012 , 98-115	0.9	22
55	Maliciously Secure Oblivious Linear Function Evaluation with Constant Overhead. <i>Lecture Notes in Computer Science</i> , 2017 , 629-659	0.9	21
54	Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO 2017 ,		21
53	Isolated Proofs of Knowledge and Isolated Zero Knowledge 2008 , 509-526		21
52	Rate-1, Linear Time and Additively Homomorphic UC Commitments. <i>Lecture Notes in Computer Science</i> , 2016 , 179-207	0.9	21
51	A Threshold Pseudorandom Function Construction and Its Applications. <i>Lecture Notes in Computer Science</i> , 2002 , 401-416	0.9	21
50	Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures. <i>Lecture Notes in Computer Science</i> , 2019 , 510-539	0.9	19
49	A Tamper and Leakage Resilient von Neumann Architecture. <i>Lecture Notes in Computer Science</i> , 2015 , 579-603	0.9	19
48	On the Complexity of Additively Homomorphic UC Commitments. <i>Lecture Notes in Computer Science</i> , 2016 , 542-565	0.9	19

47	Fast and Maliciously Secure Two-Party Computation Using the GPU. <i>Lecture Notes in Computer Science</i> , 2013 , 339-356	0.9	18
46	A Framework for Outsourcing of Secure Computation 2014 ,		17
45	Lower and Upper Bounds for Deniable Public-Key Encryption. <i>Lecture Notes in Computer Science</i> , 2011 , 125-142	0.9	17
44	Compact VSS and Efficient Homomorphic UC Commitments. <i>Lecture Notes in Computer Science</i> , 2014 , 213-232	0.9	17
43	Additively Homomorphic UC Commitments with Optimal Amortized Overhead. <i>Lecture Notes in Computer Science</i> , 2015 , 495-515	0.9	17
42	On the Communication Required for Unconditionally Secure Multiplication. <i>Lecture Notes in Computer Science</i> , 2016 , 459-488	0.9	17
41	Asynchronous Multi-Party Computation with Quadratic Communication. <i>Lecture Notes in Computer Science</i> , 2008 , 473-485	0.9	16
40	From Passive to Covert Security at Low Cost. <i>Lecture Notes in Computer Science</i> , 2010 , 128-145	0.9	16
39	Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security. <i>Lecture Notes in Computer Science</i> , 2002 , 449-464	0.9	16
38	Essentially Optimal Universally Composable Oblivious Transfer. <i>Lecture Notes in Computer Science</i> , 2009 , 318-335	0.9	15
37	Universally Composable Multiparty Computation with Partially Isolated Parties. <i>Lecture Notes in Computer Science</i> , 2009 , 315-331	0.9	15
36	Continuously Non-malleable Codes with Split-State Refresh. <i>Lecture Notes in Computer Science</i> , 2018 , 121-139	0.9	12
35	Faster Maliciously Secure Two-Party Computation Using the GPU. <i>Lecture Notes in Computer Science</i> , 2014 , 358-379	0.9	12
34	Fully Simulatable Quantum-Secure Coin-Flipping and Applications. <i>Lecture Notes in Computer Science</i> , 2011 , 21-40	0.9	12
33	Leakage-Resilient Signatures with Graceful Degradation. <i>Lecture Notes in Computer Science</i> , 2014 , 362-379		12
32	On the theoretical gap between synchronous and asynchronous MPC protocols 2010 ,		11
31	Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation. <i>Lecture Notes in Computer Science</i> , 2015 , 456-468	0.9	11
30	Predictable Arguments of Knowledge. <i>Lecture Notes in Computer Science</i> , 2017 , 121-150	0.9	11

29	YOSO: You Only Speak Once. <i>Lecture Notes in Computer Science</i> , 2021 , 64-93	0.9	11
28	On the Necessary and Sufficient Assumptions for UC Computation. <i>Lecture Notes in Computer Science</i> , 2010 , 109-127	0.9	10
27	On the Number of Synchronous Rounds Sufficient for Authenticated Byzantine Agreement. <i>Lecture Notes in Computer Science</i> , 2009 , 449-463	0.9	10
26	TARDIS: A Foundation of Time-Lock Puzzles in UC. <i>Lecture Notes in Computer Science</i> , 2021 , 429-459	0.9	10
25	Privacy-Enhancing Auctions Using Rational Cryptography. <i>Lecture Notes in Computer Science</i> , 2009 , 541-558	0.9	9
24	Upper Bounds on the Communication Complexity of Optimally Resilient Cryptographic Multiparty Computation. <i>Lecture Notes in Computer Science</i> , 2005 , 79-99	0.9	9
23	On the Connection between Leakage Tolerance and Adaptive Security. <i>Lecture Notes in Computer Science</i> , 2013 , 497-515	0.9	8
22	Reverse Firewalls for Actively Secure MPCs. <i>Lecture Notes in Computer Science</i> , 2020 , 732-762	0.9	8
21	DUPLO 2017 ,		7
20	Secure Key Management in the Cloud. <i>Lecture Notes in Computer Science</i> , 2013 , 270-289	0.9	7
19	Afgjort: A Partially Synchronous Finality Layer for Blockchains. <i>Lecture Notes in Computer Science</i> , 2020 , 24-44	0.9	7
18	Signature Schemes Secure Against Hard-to-Invert Leakage. <i>Journal of Cryptology</i> , 2016 , 29, 422-455	2.1	6
17	Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model. <i>Theoretical Computer Science</i> , 2017 , 660, 23-56	1.1	6
16	Continuous Non-Malleable Codes in the 8-Split-State Model. <i>Lecture Notes in Computer Science</i> , 2019 , 531-561	0.9	6
15	Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing. <i>Lecture Notes in Computer Science</i> , 2019 , 61-84	0.9	6
14	Secure Protocols with Asymmetric Trust 2007 , 357-375		5
13	Non-malleable Codes with Split-State Refresh. <i>Lecture Notes in Computer Science</i> , 2017 , 279-309	0.9	5
12	On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation. <i>Lecture Notes in Computer Science</i> , 2015 , 87-104	0.9	4

11	Cross and Clean: Amortized Garbled Circuits with Constant Overhead. <i>Lecture Notes in Computer Science</i> , 2016 , 582-603	0.9	4
10	Unconditionally Secure Computation with Reduced Interaction. <i>Lecture Notes in Computer Science</i> , 2016 , 420-447	0.9	4
9	Improved Non-Committing Encryption Schemes based on a General Complexity Assumption. <i>BRICS Report Series</i> , 2000 , 7,		3
8	Adaptive versus Static Security in the UC Model. <i>Lecture Notes in Computer Science</i> , 2014 , 10-28	0.9	3
7	On the Computational Overhead of MPC with Dishonest Majority. <i>Lecture Notes in Computer Science</i> , 2017 , 369-395	0.9	3
6	High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer. <i>Journal of Cryptology</i> , 2021 , 34, 1	2.1	2
5	Reactive Garbling: Foundation, Instantiation, Application. <i>Lecture Notes in Computer Science</i> , 2016 , 1022-1052	0.9	1
4	Fully Leakage-Resilient Codes. <i>Lecture Notes in Computer Science</i> , 2017 , 333-358	0.9	1
3	Limits on the Power of Cryptographic Cheap Talk. <i>Lecture Notes in Computer Science</i> , 2013 , 277-297	0.9	1
2	Continuously Non-malleable Codes in the Split-State Model. <i>Journal of Cryptology</i> , 2020 , 33, 2034-2077	2.1	
1	Weight-Based Nakamoto-Style Blockchains. <i>Lecture Notes in Computer Science</i> , 2021 , 299-319	0.9	