Jesper Buus Nielsen

List of Publications by Year in Descending Order

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	High-Performance Multi-party Computation for Binary Circuits Based on Oblivious Transfer. *Journal of Cryptology*, **2021**, 34, 1	2.1	2
81	YOSO: You Only Speak Once. *Lecture Notes in Computer Science*, **2021**, 64-93	0.9	11
80	TARDIS: A Foundation of Time-Lock Puzzles in UC. *Lecture Notes in Computer Science*, **2021**, 429-459	0.9	10
79	Weight-Based Nakamoto-Style Blockchains. *Lecture Notes in Computer Science*, **2021**, 299-319	0.9	
78	Reverse Firewalls for Actively Secure MPCs. *Lecture Notes in Computer Science*, **2020**, 732-762	0.9	8
77	Afgjort: A Partially Synchronous Finality Layer for Blockchains. *Lecture Notes in Computer Science*, **2020**, 24-44	0.9	7
76	Continuously Non-malleable Codes in the Split-State Model. *Journal of Cryptology*, **2020**, 33, 2034-2077	2.1	
75	Continuous Non-Malleable Codes in the 8-Split-State Model. *Lecture Notes in Computer Science*, **2019**, 531-561	0.9	6
74	Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures. *Lecture Notes in Computer Science*, **2019**, 510-539	0.9	19
73	Communication Lower Bounds for Statistically Secure MPC, With or Without Preprocessing. *Lecture Notes in Computer Science*, **2019**, 61-84	0.9	6
72	Continuously Non-malleable Codes with Split-State Refresh. *Lecture Notes in Computer Science*, **2018**, 121-139	0.9	12
71	Yes, There is an Oblivious RAM Lower Bound!. *Lecture Notes in Computer Science*, **2018**, 523-542	0.9	39
70	Fully leakage-resilient signatures revisited: Graceful degradation, noisy leakage, and construction in the bounded-retrieval model. *Theoretical Computer Science*, **2017**, 660, 23-56	1.1	6
69	The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited. *Lecture Notes in Computer Science*, **2017**, 167-187	0.9	28
68	Maliciously Secure Oblivious Linear Function Evaluation with Constant Overhead. *Lecture Notes in Computer Science*, **2017**, 629-659	0.9	21
67	DUPLO **2017**,		7
66	Constant Round Maliciously Secure 2PC with Function-independent Preprocessing using LEGO **2017**,		21

65	Non-malleable Codes with Split-State Refresh. *Lecture Notes in Computer Science*, **2017**, 279-309	0.9	5
64	Fully Leakage-Resilient Codes. *Lecture Notes in Computer Science*, **2017**, 333-358	0.9	1
63	Predictable Arguments of Knowledge. *Lecture Notes in Computer Science*, **2017**, 121-150	0.9	11
62	On the Computational Overhead of MPC with Dishonest Majority. *Lecture Notes in Computer Science*, **2017**, 369-395	0.9	3
61	Signature Schemes Secure Against Hard-to-Invert Leakage. *Journal of Cryptology*, **2016**, 29, 422-455	2.1	6
60	On the Complexity of Additively Homomorphic UC Commitments. *Lecture Notes in Computer Science*, **2016**, 542-565	0.9	19
59	On the Communication Required for Unconditionally Secure Multiplication. *Lecture Notes in Computer Science*, **2016**, 459-488	0.9	17
58	Rate-1, Linear Time and Additively Homomorphic UC Commitments. *Lecture Notes in Computer Science*, **2016**, 179-207	0.9	21
57	Cross and Clean: Amortized Garbled Circuits with Constant Overhead. *Lecture Notes in Computer Science*, **2016**, 582-603	0.9	4
56	Reactive Garbling: Foundation, Instantiation, Application. *Lecture Notes in Computer Science*, **2016**, 1022-1052	0.9	1
55	Unconditionally Secure Computation with Reduced Interaction. *Lecture Notes in Computer Science*, **2016**, 420-447	0.9	4
54	On the Orthogonal Vector Problem and the Feasibility of Unconditionally Secure Leakage-Resilient Computation. *Lecture Notes in Computer Science*, **2015**, 87-104	0.9	4
53	Additively Homomorphic UC Commitments with Optimal Amortized Overhead. *Lecture Notes in Computer Science*, **2015**, 495-515	0.9	17
52	A Tamper and Leakage Resilient von Neumann Architecture. *Lecture Notes in Computer Science*, **2015**, 579-603	0.9	19
51	Privacy-Free Garbled Circuits with Applications to Efficient Zero-Knowledge. *Lecture Notes in Computer Science*, **2015**, 191-219	0.9	34
50	Mind Your Coins: Fully Leakage-Resilient Signatures with Graceful Degradation. *Lecture Notes in Computer Science*, **2015**, 456-468	0.9	11
49	Secure Multiparty Computation and Secret Sharing **2015**,		193
48	A Framework for Outsourcing of Secure Computation **2014**,		17

47	Superposition Attacks on Cryptographic Protocols. *Lecture Notes in Computer Science*, **2014**, 142-161	0.9	24
46	Faster Maliciously Secure Two-Party Computation Using the GPU. *Lecture Notes in Computer Science* , **2014**, 358-379	0.9	12
45	Adaptive versus Static Security in the UC Model. *Lecture Notes in Computer Science*, **2014**, 10-28	0.9	3
44	Continuous Non-malleable Codes. *Lecture Notes in Computer Science*, **2014**, 465-488	0.9	74
43	Leakage-Resilient Signatures with Graceful Degradation. *Lecture Notes in Computer Science*, **2014**, 362-379	0.9	12
42	Compact VSS and Efficient Homomorphic UC Commitments. *Lecture Notes in Computer Science*, **2014**, 213-232	0.9	17
41	On the Connection between Leakage Tolerance and Adaptive Security. *Lecture Notes in Computer Science*, **2013**, 497-515	0.9	8
40	Secure Key Management in the Cloud. *Lecture Notes in Computer Science*, **2013**, 270-289	0.9	7
39	MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions. *Lecture Notes in Computer Science*, **2013**, 537-556	0.9	42
38	Fast and Maliciously Secure Two-Party Computation Using the GPU. *Lecture Notes in Computer Science*, **2013**, 339-356	0.9	18
37	Limits on the Power of Cryptographic Cheap Talk. *Lecture Notes in Computer Science*, **2013**, 277-297	0.9	1
36	A New Approach to Practical Active-Secure Two-Party Computation. *Lecture Notes in Computer Science*, **2012**, 681-700	0.9	206
35	Actively Secure Two-Party Evaluation of Any Quantum Operation. *Lecture Notes in Computer Science*, **2012**, 794-811	0.9	34
34	Signature Schemes Secure against Hard-to-Invert Leakage. *Lecture Notes in Computer Science*, **2012**, 98-115	0.9	22
33	Perfectly Secure Oblivious RAM without Random Oracles. *Lecture Notes in Computer Science*, **2011**, 144-163	0.9	72
32	Fully Simulatable Quantum-Secure Coin-Flipping and Applications. *Lecture Notes in Computer Science*, **2011**, 21-40	0.9	12
31	Lower and Upper Bounds for Deniable Public-Key Encryption. *Lecture Notes in Computer Science*, **2011**, 125-142	0.9	17
30	On the theoretical gap between synchronous and asynchronous MPC protocols **2010**,		11

29	A generalization of Paillier's public-key system with applications to electronic voting. *International Journal of Information Security*, **2010**, 9, 371-385	2.8	76
28	On the Necessary and Sufficient Assumptions for UC Computation. *Lecture Notes in Computer Science*, **2010**, 109-127	0.9	10
27	From Passive to Covert Security at Low Cost. *Lecture Notes in Computer Science*, **2010**, 128-145	0.9	16
26	Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries. *Lecture Notes in Computer Science*, **2010**, 685-706	0.9	28
25	Essentially Optimal Universally Composable Oblivious Transfer. *Lecture Notes in Computer Science*, **2009**, 318-335	0.9	15
24	Universally Composable Multiparty Computation with Partially Isolated Parties. *Lecture Notes in Computer Science*, **2009**, 315-331	0.9	15
23	LEGO for Two-Party Secure Computation. *Lecture Notes in Computer Science*, **2009**, 368-386	0.9	79
22	Asynchronous Multiparty Computation: Theory and Implementation. *Lecture Notes in Computer Science*, **2009**, 160-179	0.9	93
21	Secure Multiparty Computation Goes Live. *Lecture Notes in Computer Science*, **2009**, 325-343	0.9	245
20	Privacy-Enhancing Auctions Using Rational Cryptography. *Lecture Notes in Computer Science*, **2009**, 541-558	0.9	9
19	On the Number of Synchronous Rounds Sufficient for Authenticated Byzantine Agreement. *Lecture Notes in Computer Science*, **2009**, 449-463	0.9	10
18	Asynchronous Multi-Party Computation with Quadratic Communication. *Lecture Notes in Computer Science*, **2008**, 473-485	0.9	16
17	OT-Combiners via Secure Computation. *Lecture Notes in Computer Science*, **2008**, 393-411	0.9	49
16	Isolated Proofs of Knowledge and Isolated Zero Knowledge **2008**, 509-526		21
15	Scalable Multiparty Computation with Nearly Optimal Work and Resilience. *Lecture Notes in Computer Science*, **2008**, 241-261	0.9	59
14	Scalable and Unconditionally Secure Multiparty Computation **2007**, 572-590		95
13	Secure Protocols with Asymmetric Trust **2007**, 357-375		5
12	Simplified Threshold RSA with Adaptive and Proactive Security. *Lecture Notes in Computer Science*, **2006**, 593-611	0.9	31

11	Unconditionally Secure Constant-Rounds Multi-party Computation for Equality, Comparison, Bits and Exponentiation. *Lecture Notes in Computer Science*, **2006**, 285-304	0.9	194
10	Robust Multiparty Computation with Linear Communication Complexity. *Lecture Notes in Computer Science*, **2006**, 463-482	0.9	26
9	Cryptographic Asynchronous Multi-party Computation with Optimal Resilience. *Lecture Notes in Computer Science*, **2005**, 322-340	0.9	22
8	Upper Bounds on the Communication Complexity of Optimally Resilient Cryptographic Multiparty Computation. *Lecture Notes in Computer Science*, **2005**, 79-99	0.9	9
7	Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption. *Lecture Notes in Computer Science*, **2003**, 247-264	0.9	103
6	Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor. *Lecture Notes in Computer Science*, **2002**, 581-596	0.9	92
5	A Threshold Pseudorandom Function Construction and Its Applications. *Lecture Notes in Computer Science*, **2002**, 401-416	0.9	21
4	Expanding Pseudorandom Functions; or: From Known-Plaintext Security to Chosen-Plaintext Security. *Lecture Notes in Computer Science*, **2002**, 449-464	0.9	16
3	Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. *Lecture Notes in Computer Science*, **2002**, 111-126	0.9	189
2	Improved Non-Committing Encryption Schemes based on a General Complexity Assumption. *BRICS Report Series*, **2000**, 7,		3
1	Improved Non-committing Encryption Schemes Based on a General Complexity Assumption. *Lecture Notes in Computer Science*, **2000**, 432-450	0.9	95