

Yehuda Lindell

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/6308326/publications.pdf>

Version: 2024-02-01

117
papers

7,202
citations

108046

37
h-index

107981

68
g-index

125
all docs

125
docs citations

125
times ranked

2370
citing authors

#	ARTICLE	IF	CITATIONS
1	Secure multiparty computation. Communications of the ACM, 2021, 64, 86-96.	3.3	69
2	Fast Secure Two-Party ECDSA Signing. Journal of Cryptology, 2021, 34, 1.	2.1	5
3	$\mathbb{Z}_{1/p}$ -Secure Multiparty Computation without an Honest Majority and the Best of Both Worlds. Journal of Cryptology, 2020, 33, 1659-1731.	2.1	3
4	Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest. , 2019, , .		20
5	Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ. Journal of Cryptology, 2019, 32, 1026-1069.	2.1	12
6	Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme. Lecture Notes in Computer Science, 2019, , 192-210.	1.0	9
7	On the Feasibility of Extending Oblivious Transfer. Journal of Cryptology, 2018, 31, 737-773.	2.1	1
8	Fast Garbling of Circuits Under Standard Assumptions. Journal of Cryptology, 2018, 31, 798-844.	2.1	15
9	Completeness for Symmetric Two-Party Functionalities: Revisited. Journal of Cryptology, 2018, 31, 671-697.	2.1	1
10	Privacy-Preserving Search of Similar Patients in Genomic Data. Proceedings on Privacy Enhancing Technologies, 2018, 2018, 104-124.	2.3	29
11	Generalizing the SPDZ Compiler For Other Protocols. , 2018, , .		24
12	An End-to-End System for Large Scale P2P MPC-as-a-Service and Low-Bandwidth MPC for Weak Participants. , 2018, , .		20
13	Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody. , 2018, , .		90
14	Fast Large-Scale Honest-Majority MPC for Malicious Adversaries. Lecture Notes in Computer Science, 2018, , 34-64.	1.0	87
15	Fast Distributed RSA Key Generation for Semi-honest and Malicious Adversaries. Lecture Notes in Computer Science, 2018, , 331-361.	1.0	25
16	Fast Garbling of Circuits over 3-Valued Logic. Lecture Notes in Computer Science, 2018, , 620-643.	1.0	2
17	A Full Proof of the BCW Protocol for Perfectly Secure Multiparty Computation. Journal of Cryptology, 2017, 30, 58-151.	2.1	48
18	High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority. Lecture Notes in Computer Science, 2017, , 225-255.	1.0	84

#	ARTICLE	IF	CITATIONS
19	More Efficient Oblivious Transfer Extensions. <i>Journal of Cryptology</i> , 2017, 30, 805-858.	2.1	31
20	Fast Secure Two-Party ECDSA Signing. <i>Lecture Notes in Computer Science</i> , 2017, , 613-644.	1.0	89
21	Efficient Scalable Constant-Round MPC via Garbled Circuits. <i>Lecture Notes in Computer Science</i> , 2017, , 471-498.	1.0	17
22	Secure Two-Party Computation with Fairness - A Necessary Design Principle. <i>Lecture Notes in Computer Science</i> , 2017, , 565-580.	1.0	4
23	A Framework for Constructing Fast MPC over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority. , 2017, , .		57
24	Optimized Honest-Majority MPC for Malicious Adversaries â€” Breaking the 1 Billion-Gate Per Second Barrier. , 2017, , .		77
25	Fairness Versus Guaranteed Output Delivery in Secure Multiparty Computation. <i>Journal of Cryptology</i> , 2017, 30, 1157-1186.	2.1	24
26	Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. , 2017, , .		14
27	How to Simulate It â€” A Tutorial on the Simulation Proof Technique. <i>Information Security and Cryptography</i> , 2017, , 277-346.	0.2	125
28	High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. , 2016, , .		217
29	Optimizing Semi-Honest Secure Multiparty Computation for the Internet. , 2016, , .		52
30	Attribute-based Key Exchange with General Policies. , 2016, , .		12
31	Fast Cut-and-Choose-Based Protocols for Malicious and Covert Adversaries. <i>Journal of Cryptology</i> , 2016, 29, 456-490.	2.1	41
32	More Efficient Constant-Round Multi-party Computation from BMR and SHE. <i>Lecture Notes in Computer Science</i> , 2016, , 554-581.	1.0	34
33	Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries. , 2015, , .		44
34	Fast Garbling of Circuits Under Standard Assumptions. , 2015, , .		41
35	GCM-SIV. , 2015, , .		48
36	Adaptively Secure Computation with Partial Erasures. , 2015, , .		8

#	ARTICLE	IF	CITATIONS
37	Efficient Constant Round Multi-party Computation Combining BMR and SPDZ. Lecture Notes in Computer Science, 2015, , 319-338.	1.0	69
38	An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. Journal of Cryptology, 2015, 28, 312-350.	2.1	21
39	An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle. Lecture Notes in Computer Science, 2015, , 93-109.	1.0	39
40	More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. Lecture Notes in Computer Science, 2015, , 673-701.	1.0	56
41	A Simpler Variant of Universally Composable Security for Standard Multiparty Computation. Lecture Notes in Computer Science, 2015, , 3-22.	1.0	46
42	Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings. Lecture Notes in Computer Science, 2014, , 476-494.	1.0	45
43	Fairness versus Guaranteed Output Delivery in Secure Multiparty Computation. Lecture Notes in Computer Science, 2014, , 466-485.	1.0	27
44	A Note on Constant-Round Zero-Knowledge Proofs of Knowledge. Journal of Cryptology, 2013, 26, 638-654.	2.1	11
45	More efficient oblivious transfer and extensions for faster secure computation. , 2013, , .		231
46	A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness. Lecture Notes in Computer Science, 2013, , 243-262.	1.0	18
47	On the Feasibility of Extending Oblivious Transfer. Lecture Notes in Computer Science, 2013, , 519-538.	1.0	14
48	Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries. Lecture Notes in Computer Science, 2013, , 1-17.	1.0	85
49	Fair and Efficient Secure Multiparty Computation with Reputation Systems. Lecture Notes in Computer Science, 2013, , 201-220.	1.0	21
50	Hiding the Input-Size in Secure Two-Party Computation. Lecture Notes in Computer Science, 2013, , 421-440.	1.0	14
51	Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. Journal of Cryptology, 2012, 25, 680-722.	2.1	71
52	Completeness for Symmetric Two-Party Functionalities - Revisited. Lecture Notes in Computer Science, 2012, , 116-133.	1.0	5
53	Black-Box Constructions of Protocols for Secure Computation. SIAM Journal on Computing, 2011, 40, 225-266.	0.8	34
54	On Achieving the "Best of Both Worlds" in Secure Multiparty Computation. SIAM Journal on Computing, 2011, 40, 122-141.	0.8	23

#	ARTICLE	IF	CITATIONS
55	Perfectly-Secure Multiplication for Any $n/3$. Lecture Notes in Computer Science, 2011, , 240-258.	1.0	11
56	Utility Dependence in Correct and Fair Rational Secret Sharing. Journal of Cryptology, 2011, 24, 157-202.	2.1	35
57	Impossibility Results for Universal Composability in Public-Key Models and with Fixed Inputs. Journal of Cryptology, 2011, 24, 517-544.	2.1	13
58	Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. Journal of Cryptology, 2011, 24, 761-799.	2.1	14
59	Secure Computation Without Authentication. Journal of Cryptology, 2011, 24, 720-760.	2.1	12
60	Complete Fairness in Secure Two-Party Computation. Journal of the ACM, 2011, 58, 1-37.	1.8	46
61	Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. Lecture Notes in Computer Science, 2011, , 329-346.	1.0	103
62	On the Black-Box Complexity of Optimally-Fair Coin Tossing. Lecture Notes in Computer Science, 2011, , 450-467.	1.0	31
63	Highly-Efficient Universally-Composable Commitments Based on the DDH Assumption. Lecture Notes in Computer Science, 2011, , 446-466.	1.0	55
64	The IPS Compiler: Optimizations, Variants and Concrete Efficiency. Lecture Notes in Computer Science, 2011, , 259-276.	1.0	31
65	$1/p$ -Secure Multiparty Computation without Honest Majority and the Best of Both Worlds. Lecture Notes in Computer Science, 2011, , 277-296.	1.0	35
66	Secure Computation on the Web: Computing without Simultaneous Interaction. Lecture Notes in Computer Science, 2011, , 132-150.	1.0	95
67	Information-Theoretically Secure Protocols and Security under Composition. SIAM Journal on Computing, 2010, 39, 2090-2112.	0.8	45
68	Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. Journal of Cryptology, 2010, 23, 422-456.	2.1	54
69	Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. Journal of Cryptology, 2010, 23, 281-343.	2.1	115
70	Efficient Secure Two-Party Protocols. Information Security and Cryptography, 2010, , .	0.2	179
71	Semi-honest Adversaries. Information Security and Cryptography, 2010, , 53-80.	0.2	2
72	Malicious Adversaries. Information Security and Cryptography, 2010, , 81-108.	0.2	6

#	ARTICLE	IF	CITATIONS
73	Private Web Search with Malicious Adversaries. Lecture Notes in Computer Science, 2010, , 220-235.	1.0	24
74	Oblivious Transfer and Applications. Information Security and Cryptography, 2010, , 177-212.	0.2	0
75	Sigma Protocols and Efficient Zero-Knowledge1. Information Security and Cryptography, 2010, , 147-175.	0.2	4
76	The kth-Ranked Element. Information Security and Cryptography, 2010, , 213-226.	0.2	0
77	General Composition and Universal Composability in Secure Multiparty Computation. Journal of Cryptology, 2009, 22, 395-428.	2.1	20
78	A Proof of Security of Yao's Protocol for Two-Party Computation. Journal of Cryptology, 2009, 22, 161-188.	2.1	472
79	Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. Lecture Notes in Computer Science, 2009, , 183-201.	1.0	11
80	Collusion-Free Multiparty Computation in the Mediated Model. Lecture Notes in Computer Science, 2009, , 524-540.	1.0	23
81	Utility Dependence in Correct and Fair Rational Secret Sharing. Lecture Notes in Computer Science, 2009, , 559-576.	1.0	27
82	Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs. Journal of Cryptology, 2008, 21, 303-349.	2.1	7
83	Lower Bounds and Impossibility Results for Concurrent Self Composition. Journal of Cryptology, 2008, 21, 200-249.	2.1	23
84	Complete fairness in secure two-party computation. , 2008, , .		58
85	Constructions of truly practical secure protocols using standard smartcards. , 2008, , .		39
86	Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. , 2008, , 155-175.		156
87	Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. Lecture Notes in Computer Science, 2008, , 2-20.	1.0	82
88	Concurrent Composition of Secure Protocols in the Timing Model. Journal of Cryptology, 2007, 20, 431-492.	2.1	16
89	Concurrently-Secure Blind Signatures Without Random Oracles or Setup Assumptions. , 2007, , 323-341.		35
90	Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. , 2007, , 137-156.		121

#	ARTICLE	IF	CITATIONS
91	An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. Lecture Notes in Computer Science, 2007, , 52-78.	1.0	260
92	Lower bounds for non-black-box zero knowledge. Journal of Computer and System Sciences, 2006, 72, 321-391.	0.9	36
93	A Simpler Construction of CCA2-Secure Public-Key Encryption under General Assumptions. Journal of Cryptology, 2006, 19, 359-377.	2.1	40
94	On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. Journal of Cryptology, 2006, 19, 135-167.	2.1	63
95	Session-Key Generation Using Human Passwords Only. Journal of Cryptology, 2006, 19, 241-340.	2.1	40
96	A framework for password-based authenticated key exchange 1. ACM Transactions on Information and System Security, 2006, 9, 181-234.	4.5	70
97	Information-theoretically secure protocols and security under composition. , 2006, , .		43
98	On the composition of authenticated Byzantine Agreement. Journal of the ACM, 2006, 53, 881-917.	1.8	15
99	On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation. Lecture Notes in Computer Science, 2006, , 483-500.	1.0	30
100	Universally Composable Password-Based Key Exchange. Lecture Notes in Computer Science, 2005, , 404-421.	1.0	169
101	Secure Multi-Party Computation without Agreement. Journal of Cryptology, 2005, 18, 247-287.	2.1	82
102	Concurrent general composition of secure protocols in the timing model. , 2005, , .		25
103	Secure Computation Without Authentication. Lecture Notes in Computer Science, 2005, , 361-377.	1.0	65
104	Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs. Lecture Notes in Computer Science, 2005, , 128-149.	1.0	12
105	Strict Polynomial-Time in Simulation and Extraction. SIAM Journal on Computing, 2004, 33, 783-818.	0.8	28
106	Lower Bounds for Concurrent Self Composition. Lecture Notes in Computer Science, 2004, , 203-222.	1.0	58
107	A Statistical Theory for Quantitative Association Rules. Journal of Intelligent Information Systems, 2003, 20, 255-283.	2.8	91
108	Bounded-concurrent secure two-party computation without setup assumptions. , 2003, , .		54

#	ARTICLE	IF	CITATIONS
109	On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions. Lecture Notes in Computer Science, 2003, , 68-86.	1.0	74
110	Strict polynomial-time in simulation and extraction. , 2002, , .		41
111	Universally composable two-party and multi-party secure computation. , 2002, , .		334
112	Privacy Preserving Data Mining. Journal of Cryptology, 2002, 15, 177-206.	2.1	492
113	Secure Computation without Agreement. Lecture Notes in Computer Science, 2002, , 17-32.	1.0	50
114	Session-Key Generation Using Human Passwords Only. Lecture Notes in Computer Science, 2001, , 408-432.	1.0	136
115	From Keys to Databasesâ€”Real-World Applications of Secure Multi-Party Computation. Computer Journal, 0, , .	1.5	57
116	Introduction to Modern Cryptography. , 0, , .		497
117	Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs*. SSRN Electronic Journal, 0, , .	0.4	0